

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yasuyuki NOMIZU, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: DURABLE AND UNDECIPHERABLE DIGITAL WATERMARKING TECHNIQUE AND  
DETECTION OF UNAUTHORIZED USE

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

APPLICATION NUMBER

MONTH/DAY/YEAR

Japan

2002-338118

November 21, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)  
☐ are submitted herewith  
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

C. Irvin McClelland  
Registration Number 21,124

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。  
This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

2002年11月21日

出願番号  
Application Number:

特願2002-338118

[ST. 10/C]:

[JP 2002-338118]

出願人

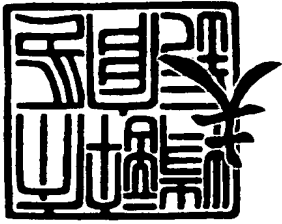
株式会社リコー

Applicant(s):

特許庁長官  
Commissioner,  
Japan Patent Office

今井 康

2003年 9月24日



【書類名】 特許願

【整理番号】 0204964

【提出日】 平成14年11月21日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06G 9/00

【発明の名称】 符号生成装置、画像処理装置、符号生成プログラム、画像処理プログラムおよび記憶媒体

【請求項の数】 47

【発明者】

【住所又は居所】 鳥取県鳥取市千代水一丁目百番地 アイシン千代ビル  
リコー鳥取技術開発株式会社内

【氏名】 西村 隆之

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 野水 泰之

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 作山 宏幸

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 原 潤一

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 松浦 熱河

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 矢野 隆則

## 【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

【氏名】 児玉 卓

## 【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

【氏名】 宮澤 利夫

## 【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

【氏名】 新海 康行

## 【特許出願人】

【識別番号】 000006747

【氏名又は名称】 株式会社リコー

【代表者】 桜井 正光

## 【代理人】

【識別番号】 100101177

## 【弁理士】

【氏名又は名称】 柏木 慎史

【電話番号】 03(5333)4133

## 【選任した代理人】

【識別番号】 100102130

## 【弁理士】

【氏名又は名称】 小山 尚人

【電話番号】 03(5333)4133

## 【選任した代理人】

【識別番号】 100072110

## 【弁理士】

【氏名又は名称】 柏木 明

【電話番号】 03(5333)4133

## 【手数料の表示】

【予納台帳番号】 063027

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9808802

【包括委任状番号】 0004335

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 符号生成装置、画像処理装置、符号生成プログラム、画像処理プログラムおよび記憶媒体

【特許請求の範囲】

【請求項 1】 画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、

前記量子化係数をブロック単位に分割するブロック分割手段と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換手段と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割手段と、

n 番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n 番目の前記ブロックの m 番目のビットプレーンの N (N は偶数) 個の有意ビット  $Q_{nm}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数 T との関係が、(1) 式で表わされる ON 状態または (2) 式で表わされる OFF 状態を満足するように前記有意ビットの ON/OFF を調整する電子透かし埋め込み手段と、

ON/OFF を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、  
を具備する符号生成装置。

【数 1】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| > T \quad \dots (1)$$

【数 2】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| > T \quad \dots (2)$$

【請求項2】 画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、

前記量子化係数をブロック単位に分割するブロック分割手段と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換手段と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割手段と、

n 番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n 番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(3) 式で表わされる  $ON$  状態または (4) 式で表わされる  $OFF$  状態を満足するように前記有意ビットの  $ON/OFF$  を調整する電子透かし埋め込み手段と、

$ON/OFF$  を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、

を具備する符号生成装置。

【数3】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| > T \quad \dots (3)$$

【数4】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| > T \quad \dots (4)$$

【請求項3】 画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、

前記量子化係数をブロック単位に分割するブロック分割手段と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロッ

ク毎に符号化ハッシュ値を取得するハッシュ変換手段と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割手段と、

$n_i$  番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、 $n_i$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(5) 式で表わされる  $ON$  状態または (6) 式で表わされる  $OFF$  状態を満足するように前記有意ビットの  $ON/OFF$  を調整する電子透かし埋め込み手段と、

$ON/OFF$  を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、

を具備する符号生成装置。

【数 5】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i_k, i_k) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i_k, i_k) \right| > T$$

... (5)

【数 6】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i_k, i_k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i_k, i_k) \right| > T$$

... (6)

【請求項 4】 前記電子透かし埋め込み手段は、前記符号化ハッシュ値が偶数である場合に  $N$  個の前記有意ビットによって形成される情報と自然数  $T$  との関係を  $ON$  状態とし前記符号化ハッシュ値が奇数である場合に  $N$  個の前記有意ビットによって形成される情報と自然数  $T$  との関係を  $OFF$  状態とする第 1 の方式、または、前記符号化ハッシュ値が奇数である場合に  $N$  個の前記有意ビットによって形成される情報と自然数  $T$  との関係を  $ON$  状態とし前記符号化ハッシュ値が偶数である場合に  $N$  個の前記有意ビットによって形成される情報と自然数  $T$  との関係を  $OFF$  状態とする第 2 の方式のいずれかの方式により前記有意ビットの  $ON$



／OFFを調整する請求項1ないし3のいずれかーに記載の符号生成装置。

【請求項5】 前記第1の方式と前記第2の方式とのいずれか一方を切替自在に設定する方式設定手段を具備し、

前記電子透かし埋め込み手段は、前記方式設定手段が設定した方式にしたがって偶奇性を合わせる請求項4記載の符号生成装置。

【請求項6】 前記方式設定手段は、前記符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて、前記第1の方式または前記第2の方式を設定する請求項5記載の符号生成装置。

【請求項7】 前記方式設定手段は、前記符号化ハッシュ値と外部から入力された秘密情報とに基づいて、前記第1の方式または前記第2の方式を設定する請求項5記載の符号生成装置。

【請求項8】 前記符号化手段は、上位のビットプレーンから下位のビットプレーン方向へ符号化を行ない、OFFビットをONにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをOFFにし、ONビットをOFFにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをONにする請求項1ないし7のいずれかーに記載の符号生成装置。

【請求項9】 前記量子化係数を選択的に取得する量子化係数選択手段を具備し、

前記電子透かし埋め込み手段は、選択的に取得した前記量子化係数における前記有意ビットのON／OFFを行なう請求項1ないし8のいずれかーに記載の符号生成装置。

【請求項10】 前記量子化係数選択手段は、隣り合う前記量子化係数との差がしきい値以上である前記量子化係数を選択する請求項9記載の符号生成装置。

【請求項11】 前記しきい値は調整可能である請求項10記載の符号生成装置。

【請求項12】 前記量子化係数に前記しきい値を埋め込むしきい値埋め込み手段を具備し、

前記符号化手段は、前記しきい値を埋め込んだ前記量子化係数を符号化する請求項 10 または 11 記載の符号生成装置。

【請求項 13】 前記量子化係数選択手段が取得する前記量子化係数の取得頻度は調整可能である請求項 9 ないし 12 のいずれかーに記載の符号生成装置。

【請求項 14】 秘密入力情報を入力する秘密情報入力手段を具備し、  
前記ハッシュ変換手段は、前記量子化係数に加えて、前記秘密情報に基づいてハッシュ変換を行なう請求項 1 ないし 13 のいずれかーに記載の符号生成装置。

【請求項 15】 日付情報を取得する日付情報取得手段を具備し、  
前記ハッシュ変換手段は、前記量子化係数に加えて、前記日付情報に基づいてハッシュ変換を行なう請求項 1 ないし 13 のいずれかーに記載の符号生成装置。

【請求項 16】 装置の製造番号を認識する製造番号認識手段を具備し、  
前記ハッシュ変換手段は、前記量子化係数に加えて、前記製造番号に基づく情報に基づいてハッシュ変換を行なう請求項 1 ないし 13 のいずれかーに記載の符号生成装置。

【請求項 17】 秘密入力情報を入力する秘密情報入力手段と、  
日付情報を取得する日付情報取得手段と、  
装置の製造番号を認識する製造番号認識手段と、  
を具備し、  
前記ハッシュ変換手段は、前記量子化係数に加えて、前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報に基づいてハッシュ変換を行なう請求項 1 ないし 13 のいずれかーに記載の符号生成装置。

【請求項 18】 前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報を選択する選択手段を具備し、  
前記ハッシュ変換手段は、選択した前記情報に基づいてハッシュ変換を行なう請求項 17 記載の符号生成装置。

【請求項 19】 対象画像を光学的に読み取った画像を入力する画像入力手段を具備し、

前記量子化手段は、前記画像入力手段が入力した画像を量子化する請求項 1 ないし 18 のいずれかーに記載の符号生成装置。

【請求項 20】 請求項 1 ないし 19 のいずれか一に記載の符号生成装置の符号化手段が生成した符号列データを復号化して量子化係数を生成する復号化手段と、

前記量子化係数をブロック単位に分割する復号ブロック分割手段と、

前記各ブロックの量子化係数に基づいてハッシュ変換を行ないブロック毎に復号化ハッシュ値を取得する復号ハッシュ変換手段と、

前記各ブロックの量子化係数をビットプレーン単位に分割する復号ビットプレーン分割手段と、

$n_i$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が (7) 式を満足する  $ON$  状態および (8) 式を満足する  $OFF$  状態によって表わされる偶奇性と、 $n_i$  番目の前記ブロックにおける復号化ハッシュ値の偶奇性と、が一致するか否かを判断する流用検出手段と、

を具備する画像処理装置。

【数 7】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i k, i k) \right| > \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i k, i k) \right| \quad \dots (7)$$

【数 8】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i k, i k) \right| < \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i k, i k) \right| \quad \dots (8)$$

【請求項 21】 前記量子化係数を離散ウェーブレット変換して画像データを生成する画像生成手段と、

偶奇性が一致した前記ブロック位置を記憶する流用位置記憶手段と、

前記画像データに基づく画像を、記憶した前記ブロック位置を強調して表示部に表示させる強調表示手段と、

を具備する請求項 20 記載の発明の画像処理装置。

【請求項 2 2】 前記強調表示手段は、記憶した前記ブロック位置を単色で表示させる請求項 2 1 記載の画像処理装置。

【請求項 2 3】 前記強調表示手段は、記憶した前記ブロック位置を反転表示させる請求項 2 1 記載の画像処理装置。

【請求項 2 4】 コンピュータにインストールされ、このコンピュータに、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化機能と、

前記量子化係数をブロック単位に分割するブロック分割機能と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換機能と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割機能と、

n 番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n 番目の前記ブロックの m 番目のビットプレーンの N (N は偶数) 個の有意ビット  $Q_{nm}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数 T との関係が、(1) 式で表わされる ON 状態または (2) 式で表わされる OFF 状態を満足するように前記有意ビットの ON/OFF を調整する電子透かし埋め込み機能と、

ON/OFF を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化機能と、  
を実行させる符号生成プログラム。

【数 9】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| > T \quad \dots (1)$$

【数 10】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| > T$$

... (2)

【請求項 25】 コンピュータにインストールされ、このコンピュータに、  
画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化  
した量子化係数を生成する量子化機能と、

前記量子化係数をブロック単位に分割するブロック分割機能と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロッ  
ク毎に符号化ハッシュ値を取得するハッシュ変換機能と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割機能と、

n 番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n 番目の  
前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と  
自然数  $T$  との関係が、(3) 式で表わされる  $ON$  状態または (4) 式で表わされ  
る  $OFF$  状態を満足するように前記有意ビットの  $ON/OFF$  を調整する電子透  
かし埋め込み機能と、

$ON/OFF$  を調整した前記有意ビットを含む前記量子化係数を符号化して符  
号列データを生成する符号化機能と、  
を実行させる符号生成プログラム。

【数 11】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| > T$$

... (3)

【数 1 2】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| > T$$

... (4)

【請求項 26】 コンピュータにインストールされ、このコンピュータに、  
画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化  
した量子化係数を生成する量子化機能と、

前記量子化係数をブロック単位に分割するブロック分割機能と、

前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロッ  
ク毎に符号化ハッシュ値を取得するハッシュ変換機能と、

前記各ブロックをビットプレーン単位に分割するビットプレーン分割機能と、

$n_i$  番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、 $n_i$  番  
目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  
 $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される  
情報と自然数  $T$  との関係が、(5) 式で表わされる  $ON$  状態または (6) 式で表  
わされる  $OFF$  状態を満足するように前記有意ビットの  $ON/OFF$  を調整する  
電子透かし埋め込み機能と、

$ON/OFF$  を調整した前記有意ビットを含む前記量子化係数を符号化して符  
号列データを生成する符号化機能と、

を実行させる符号生成プログラム。

【数 1 3】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| > T$$

... (5)

【数 14】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| > T$$

... (6)

【請求項 27】 前記電子透かし埋め込み機能は、前記符号化ハッシュ値が偶数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をON状態とし前記符号化ハッシュ値が奇数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をOFF状態とする第1の方式、または、前記符号化ハッシュ値が奇数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をON状態とし前記符号化ハッシュ値が偶数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をOFF状態とする第2の方式のいずれかの方式により前記有意ビットのON/OFFを調整する請求項 24 ないし 26 のいずれかーに記載の符号生成プログラム。

【請求項 28】 前記第1の方式と前記第2の方式とのいずれか一方を切替自在に設定する方式設定機能を前記コンピュータに実行させ、

前記電子透かし埋め込み機能は、設定された方式にしたがって偶奇性を合わせる請求項 27 記載の符号生成プログラム。

【請求項 29】 前記方式設定機能は、前記符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて、前記第1の方式または前記第2の方式を設定する請求項 28 記載の符号生成プログラム。

【請求項 30】 前記方式設定機能は、前記符号化ハッシュ値と外部から入力された秘密情報とに基づいて、前記第1の方式または前記第2の方式を設定する請求項 28 記載の符号生成プログラム。

【請求項 31】 前記符号化機能は、上位のビットプレーンから下位のビットプレーン方向へ符号化を行ない、OFFビットをONにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをOFFにし、ONビットをOFFにする場合は処理対象となるビットプレーンの下位ビッ

トプレーン内の該当する全てのビットを ON にした符号列データを生成する請求項 2 4 ないし 3 0 のいずれかに記載の符号生成プログラム。

【請求項 3 2】 前記量子化係数を選択的に取得する量子化係数選択機能を前記コンピュータに実行させ、

前記電子透かし埋め込み手段は、選択的に取得した前記量子化係数における前記有意ビットの ON / OFF を行なう請求項 2 4 ないし 3 1 のいずれかに記載の符号生成プログラム。

【請求項 3 3】 前記量子化係数選択機能により選択する前記量子化係数は、隣り合う前記量子化係数との差がしきい値以上である前記量子化係数である請求項 3 2 記載の符号生成プログラム。

【請求項 3 4】 前記しきい値は調整可能である請求項 3 3 記載の符号生成プログラム。

【請求項 3 5】 前記量子化係数に前記しきい値を埋め込むしきい値埋め込み機能を前記コンピュータに実行させ、

前記符号化機能は、前記しきい値を埋め込んだ前記量子化係数を符号化した符号列データを生成する請求項 3 3 または 3 4 記載の符号生成装置。

【請求項 3 6】 前記量子化係数選択機能により取得する前記量子化係数の取得頻度は調整可能である請求項 3 2 ないし 3 5 のいずれかに記載の符号生成プログラム。

【請求項 3 7】 前記ハッシュ変換機能は、前記量子化係数に加えて、外部から入力された秘密情報に基づいてハッシュ変換を行なう請求項 2 4 ないし 3 6 のいずれかに記載の符号生成プログラム。

【請求項 3 8】 前記ハッシュ変換機能は、前記量子化係数に加えて、日付情報に基づいてハッシュ変換を行なう請求項 2 4 ないし 3 6 のいずれかに記載の符号生成プログラム。

【請求項 3 9】 前記ハッシュ変換機能は、前記量子化係数に加えて、装置の製造番号に基づく情報に基づいてハッシュ変換を行なう請求項 2 4 ないし 3 6 のいずれかに記載の符号生成プログラム。

【請求項 4 0】 前記ハッシュ変換機能は、前記量子化係数に加えて、外部



から入力された秘密情報、日付情報、装置の製造番号に基づく情報のうち二つ以上の情報に基づいてハッシュ変換を行なう請求項 24 ないし 36 のいずれかに記載の符号生成プログラム。

【請求項 41】 前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報を選択する選択機能を前記コンピュータに実行させ、

前記ハッシュ変換機能は、選択した前記情報に基づいてハッシュ変換を行なう請求項 40 記載の符号生成プログラム。

【請求項 42】 コンピュータにインストールされ、このコンピュータに、請求項 24 ないし 41 のいずれかに記載の符号生成プログラムの実行により生成した符号列データを復号化して量子化係数を生成する復号化機能と、

前記量子化係数をブロック単位に分割する復号ブロック分割機能と、

前記各ブロックの量子化係数に基づいてハッシュ変換を行ないブロック毎に復号化ハッシュ値を取得する復号ハッシュ変換機能と、

前記各ブロックの量子化係数をビットプレーン単位に分割する復号ビットプレーン分割機能と、

$n_i$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が (7) 式を満足する  $ON$  状態および (8) 式を満足する  $OFF$  状態によって表わされる偶奇性と、 $n_i$  番目の前記ブロックにおける復号化ハッシュ値の偶奇性と、が一致するか否かを判断する流用検出機能と、

を実行させる画像処理プログラム。

【数 15】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i k, i k) \right| > \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i k, i k) \right| \quad \dots (7)$$

【数 16】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q n_k m_k(i k, i k) \right| < \left| \sum_{k=\frac{1}{2}N+1}^N Q n_k m_k(i k, i k) \right| \quad \dots (8)$$

【請求項 43】 前記量子化係数を離散ウェーブレット変換して画像データを生成する画像生成機能と、

前記画像データに基づく画像を、偶奇性が一致した前記ブロック位置を強調して表示部に表示させる強調表示機能と、

を具備する請求項 42 記載の画像処理プログラム。

【請求項 44】 前記強調表示機能は、偶奇性が一致した前記ブロック位置を単色で表示させる請求項 43 記載の画像処理プログラム。

【請求項 45】 前記強調表示機能は、偶奇性が一致した前記ブロック位置を反転表示させる請求項 43 記載の画像処理プログラム。

【請求項 46】 請求項 24 ないし 41 のいずれかに記載の符号生成プログラムを記憶し、機械読み取り可能である記憶媒体。

【請求項 47】 請求項 42 ないし 45 のいずれかに記載の画像処理プログラムを記憶し、機械読み取り可能である記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、符号生成装置、画像処理装置、符号生成プログラム、画像処理プログラムおよび記憶媒体に関する。

【0002】

【従来の技術】

デジタル画像等のデジタル情報（デジタルコンテンツ）は、コンピュータなどによって、情報を劣化させることなく、簡単にコピーすることができる。近年では、デジタル画像技術の発達にしたがって、デジタルカメラ等によって取得されたデジタル画像等を、証拠写真として使用することも可能になってきている。このようなデジタル情報には、著作権等が付され、許可無くコピーしたり、コピー

したデジタル情報を再利用したりすることが禁じられているものがある。

### 【0003】

デジタルコンテンツは、簡単にコピーすることができることに加えて、簡単な修飾処理等の操作を施して書換えなどを行なうことによって、容易に改ざんすることができる。このため、デジタル情報を不正にコピーし、不正にコピーした画像をそのまま、あるいは、若干の改ざんを加えて勝手に再利用されてしまうことがある。

### 【0004】

この対策として、デジタル画像などのデジタルコンテンツ中に該デジタルコンテンツを普通に再生した場合には視覚できない情報を付加する、いわゆる、電子透かしやデータハイディングなどと呼ばれる方法によって、デジタルコンテンツの不正利用を防止するようにした技術がある。これにより、デジタルコンテンツが不正に利用されているか否かを、該デジタルコンテンツ中に埋込まれた電子透かしによって判断することができる。

### 【0005】

このように、電子透かしをデジタルコンテンツに埋込む用途には、次のようなものがある。

- A. 著作権情報の記録
- B. 違法コピー者情報の追跡
- C. IPアドレスの履歴記録
- D. 違法コピーの防止：不可視・高耐性型
- E. 改ざん防止への応用：不可視・低耐性型
- F. 認証
- G. 秘密通信
- H. 所有権者表示のためにデジタルコンテンツの注釈やラベルを埋込む：可視・不可逆型
- I. 透かし除去可能化：可視・可逆型……コンテンツ配布

### 【0006】

その中で、例えば、デジタルコンテンツの著作権者の権利保護を目的とする“D

・ 違法コピーの防止”を実現する用途としては、次のものが考案されている。

**【0007】**

例えば、著作者情報や購入者情報などの著作権に関連する情報を透かし込んだデジタルコンテンツを販売・流通させる際に、このデジタルコンテンツを販売・流通させるコンテンツプロバイダが、著作権情報が透かし込まれていることを予め知らせ、デジタルコンテンツの購入段階において購入者に対して著作権を認識させることにより、良識ある購入者に対する不正利用を心理的に抑止する効果を狙った形態が実現されている。この形態でも、悪意ある利用者は、著作権を無視して不正利用するかもしれないが、不正利用されたデジタルコンテンツを取得し、取得したデジタルコンテンツから電子透かし情報を抽出することで、不正利用者の特定と権利主張が可能である（例えば、非特許文献1参照）。

**【0008】**

デジタルコンテンツ中に電子透かしを埋込む技術（以降、電子透かし技術という）は、大きく分類して、（1）電子透かしを内容データの標本値に直接埋込む技術と、（2）電子透かしを周波数成分に埋込む技術と、の二つに分類することができる。

**【0009】**

（1）の電子透かしをデータの標本値に埋込む方法は、デジタルコンテンツに対する加工や圧縮などの処理が軽いが、電子透かしを埋込んだデジタルコンテンツに対して加工や圧縮などの処理を行なうと、埋込まれた電子透かしが失われやすいという特性がある。

**【0010】**

これに対し、（2）の周波数成分に埋込む方法は、デジタルコンテンツに対して電子透かしを埋込んだり抽出したりする処理が重いが、電子透かしを埋込んだデジタルコンテンツに対して加工や圧縮などの処理に強いという特性がある。

**【0011】**

ところで、モノクロデジタルコピーやFAX、新聞の白黒印刷などにおいては、白黒の2値画像を利用し、元画像が欠損無く復元できるLoss-Less画像圧縮方式が推奨され、一般化されている。このようなLoss-Less画像圧縮方式としては

、例えば、国際電気通信連合（ITU-T）のG3，G4規格などで、MH，MR，MMR等がある。

【0012】

しかし、これらの方式は、中間調処理された画像や誤差拡散処理された画像などにおける符号化効率が悪く、圧縮できないことも多くある。

【0013】

このような問題を解決する方法としては、画像のエントロピーを基に符号化を行なう算術符号化方式と呼ばれる方式が注目されている。例えば、2値画像の新しい符号化方式の国際標準を検討しているグループのJBIGでは、QM-Coderと呼ばれる算術符号化方式が採用されている。このQM-Coderと呼ばれる算術符号化方式は、ITU-Tの標準として勧告化されている。

【0014】

ところで、デジタルスチルカメラやデジタルビデオカメラ等の、デジタルのカラー画像や濃淡画像などの多値画像を取り扱う製品においては、元画像の細かい情報が失われる等の少しの画質劣化は犠牲にし、保存時の圧縮効果を重要視したLossy圧縮技術を利用することが多くなっている。このようなLossy圧縮技術としては、離散コサイン変換（DCT：Discrete Cosine Transform）による周波数変換を利用したJPEGやMPEGなどがある。

【0015】

上述したJPEGの後継標準として、Lossy符号化方式とLoss-Less符号化方式との統一符号化、及び、2値データと多値データとの統一符号化方式として、現在熱い期待が寄せられているJPEG2000がある。JPEG2000では、離散ウェーブレット変換（DWT：Discrete Wavelet Transform）を使用することで高圧縮時の画質劣化を減少させるとともに、MQ-Coderを適用することで高圧縮率化を図ることができる。MQ-Coderは、上述したJBIGのQM-Coderに類似しており、JBIG2にも採用されている算術符号化方式である。

【0016】

【非特許文献1】

電子透かし技術に関する調査報告書 1999年3月：日本電子工業振興協会編より（大元：日経ビジネス：電子情報の不正コピー防止，1998年2月23日号 p p. 68-70（1998））

【0017】

【発明が解決しようとする課題】

ところで、圧縮処理を施した多値画像のデジタルコンテンツに対して電子透かしを埋め込む際に、上述した（1）の方法で電子透かしを埋め込んだ場合、デジタルコンテンツの保存に際して画像圧縮のために符号化処理を施すことにより画質が劣化する。そして、この画質劣化によって、このデジタルコンテンツ中に埋め込んだ電子透かしも劣化してしまう。このため、圧縮のための符号化および伸長のための復号化を繰り返す程、デジタルコンテンツ中に埋め込まれた電子透かしを検知する能力が弱くなり、画像中に電子透かしを埋め込んだにも拘わらず、該画像の流用を検出することが困難になってしまう。

【0018】

このようなことから、圧縮処理を施したデジタルコンテンツの保存に際して、デジタルコンテンツの流用検出を目的として電子透かしを埋め込む場合、符号化および復号化を繰り返しても該電子透かしを検出できるように、上述した“（2）圧縮のための符号列データ（周波数成分）に電子透かしを埋め込む方法”を適用するのが適切と言える。

【0019】

本発明の目的は、符号化、復号化を繰り返しても流用された画像であることを検出できるようにすることである。

【0020】

【課題を解決するための手段】

請求項1記載の発明の符号生成装置は、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、前記量子化係数をブロック単位に分割するブロック分割手段と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換手段と、前記各ブロックをビットプレーン単位

に分割するビットプレーン分割手段と、n番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n番目の前記ブロックのm番目のビットプレーンのN(Nは偶数)個の有意ビット $Q_{nm}(x, y)$  ( $x=0, 1, \dots; y=0, 1, \dots$ )によって形成される情報と自然数Tとの関係が、(1)式で表わされるON状態または(2)式で表わされるOFF状態を満足するように前記有意ビットのON/OFFを調整する電子透かし埋め込み手段と、ON/OFFを調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、を具備する。

【0021】

【数17】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| > T \quad \dots (1)$$

【0022】

【数18】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| > T \quad \dots (2)$$

【0023】

ここで、量子化係数をビット表現したビット列を上位ビットから下位ビット方向に符号化する際に、注目係数が予め“0”ではないことが解っている状態を有意であるとし、このような状態にある注目係数を有意ビットとする。有意ビットは、既に1であり符号化してあるビットをいう。

【0024】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、単一のビットプレーン内の有意ビットに対してON/OFF調整するため

、符号化に際してビットプレーン単位の切り捨てがあった場合にも、有意ビットの ON/OFF によって埋め込まれる電子透かしを消滅させることはない。さらに、有意ビットの ON/OFF 調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項 20 記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができる。

### 【0025】

請求項 2 記載の発明の符号生成装置は、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、前記量子化係数をブロック単位に分割するブロック分割手段と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換手段と、前記各ブロックをビットプレーン単位に分割するビットプレーン分割手段と、 $n$  番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、 $n$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(3) 式で表わされる ON 状態または (4) 式で表わされる OFF 状態を満足するように前記有意ビットの ON/OFF を調整する電子透かし埋め込み手段と、ON/OFF を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、を具備する。

### 【0026】

#### 【数 19】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| > T$$

... (3)

### 【0027】



【数 20】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| > T$$

... (4)

【0028】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、有意ビットの ON/OFF 調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項 20 記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができる。さらに、ON/OFF 調整する有意ビットを複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を抑制するとともに、流用の検出に際しての対象領域の分解能を上げることができる。

【0029】

請求項 3 記載の発明の符号生成装置は、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化手段と、前記量子化係数をブロック単位に分割するブロック分割手段と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換手段と、前記各ブロックをビットプレーン単位に分割するビットプレーン分割手段と、 $n_i$  番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、 $n_i$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots$ ;  $y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(5) 式で表わされる ON 状態または (6) 式で表わされる OFF 状態を満足するように前記有意ビットの ON/OFF を調整する電子透かし埋め込み手段と、ON/OFF を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化手段と、を具備する。

【0030】

【数 2 1】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i k, i k) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i k, i k) \right| > T$$

... (5)

【0 0 3 1】

【数 2 2】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i k, i k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i k, i k) \right| > T$$

... (6)

【0 0 3 2】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項20記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができる。さらに、ON/OFF調整する有意ビットを複数のブロックの複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を効果的に抑制するとともに、流用の検出に際しての対象領域の分解能をより上げることができる。

【0 0 3 3】

請求項4記載の発明は、請求項1ないし3のいずれかーに記載の符号生成装置において、前記電子透かし埋め込み手段は、前記符号化ハッシュ値が偶数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をON状態とし前記符号化ハッシュ値が奇数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をOFF状態とする第1の方式、または、前記符号化ハッシュ値が奇数である場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をON状態とし前記符号化ハッシュ値が偶数である

場合にN個の前記有意ビットによって形成される情報と自然数Tとの関係をOFF状態とする第2の方式のいずれかの方式により前記有意ビットのON/OFFを調整する。

#### 【0034】

したがって、第1の方式または第2の方式の2つの方式のうちいずれか一方を選択的に用いることにより、埋め込まれる電子透かしを、効果的に第三者に解読し難くすることができる。

#### 【0035】

請求項5記載の発明は、請求項4記載の符号生成装置において、前記第1の方式と前記第2の方式とのいずれか一方を切替自在に設定する方式設定手段を具備し、前記電子透かし埋め込み手段は、前記方式設定手段が設定した方式にしたがって偶奇性を合わせる。

#### 【0036】

したがって、第1の方式または第2の方式を切替自在に設定することができる。

#### 【0037】

請求項6記載の発明は、請求項5記載の符号生成装置において、前記方式設定手段は、前記符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて、前記第1の方式または前記第2の方式を設定する。

#### 【0038】

したがって、符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0039】

請求項7記載の発明は、請求項5記載の符号生成装置において、前記方式設定手段は、前記符号化ハッシュ値と外部から入力された秘密情報とに基づいて、前記第1の方式または前記第2の方式を設定する。

#### 【0040】

したがって、秘密情報が入力された場合には、符号化ハッシュ値と秘密情報と

に基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

【0041】

請求項8記載の発明は、請求項1ないし7のいずれかに記載の符号生成装置において、前記符号化手段は、上位のビットプレーンから下位のビットプレーン方向へ符号化を行ない、OFFビットをONにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをOFFにし、ONビットをOFFにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをONにする。

【0042】

したがって、ビットプレーンの上位から下位方向への符号化においてビットのON/OFFを均等に行ない、有意ビットのON/OFFにより電子透かしを埋め込むことによる画質劣化を抑えることができる。

【0043】

請求項9記載の発明は、請求項1ないし8のいずれかに記載の符号生成装置において、前記量子化係数を選択的に取得する量子化係数選択手段を具備し、前記電子透かし埋め込み手段は、選択的に取得した前記量子化係数における前記有意ビットのON/OFFを行なう。

【0044】

したがって、全ての量子化係数の有意ビットをON/OFF調整を行なう場合と比較して、電子透かしを埋め込むことによる画質劣化を抑えることができる。

【0045】

請求項10記載の発明は、請求項9記載の符号生成装置において、前記量子化係数選択手段は、隣り合う前記量子化係数との差がしきい値以上である前記量子化係数を選択する。

【0046】

したがって、隣り合う量子化係数との差がしきい値以上である、すなわち、隣り合う量子化係数に対して変化の激しい量子化係数における有意ビットをON/OFFすることにより、電子透かしを埋め込むことによる画質劣化をより効果的

に抑えることができる。

**【0047】**

請求項 11 記載の発明は、請求項 10 記載の符号生成装置において、前記しきい値は調整可能である。

**【0048】**

したがって、例えば、画質劣化程度や流用の検出精度等に応じて、使用目的に応じたしきい値を設定することができる。

**【0049】**

請求項 12 記載の発明は、請求項 10 または 11 記載の符号生成装置において、前記量子化係数に前記しきい値を埋め込むしきい値埋め込み手段を具備し、前記符号化手段は、前記しきい値を埋め込んだ前記量子化係数を符号化する。

**【0050】**

したがって、例えば、請求項 20 記載の発明の画像処理装置を用いて、符号列データ中に埋め込んだしきい値を復元して活用することができる。

**【0051】**

請求項 13 記載の発明は、請求項 9 ないし 12 のいずれか一に記載の符号生成装置において、前記量子化係数選択手段が取得する前記量子化係数の取得頻度を調整可能である。

**【0052】**

したがって、例えば、目的とする画質程度等に応じた頻度で量子化係数を取得することにより、電子透かしを埋め込むことによる画質劣化の程度を管理することができる。

**【0053】**

請求項 14 記載の発明は、請求項 1 ないし 13 のいずれか一に記載の符号生成装置において、秘密入力情報を入力する秘密情報入力手段を具備し、前記ハッシュ変換手段は、量子化係数に加えて、前記秘密情報に基づいてハッシュ変換を行なう。

**【0054】**

したがって、各ブロックの量子化係数に加えて秘密情報をハッシュ変換の種と

することにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0055】

請求項15記載の発明は、請求項1ないし13のいずれかに記載の符号生成装置において、日付情報を取得する日付情報取得手段を具備し、前記ハッシュ変換手段は、量子化係数に加えて、前記日付情報に基づいてハッシュ変換を行なう。

#### 【0056】

したがって、各ブロックの量子化係数に加えて日付情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0057】

請求項16記載の発明は、請求項1ないし13のいずれかに記載の符号生成装置において、装置の製造番号を認識する製造番号認識手段を具備し、前記ハッシュ変換手段は、量子化係数に加えて、前記製造番号に基づく情報に基づいてハッシュ変換を行なう。

#### 【0058】

したがって、各ブロックの量子化係数に加えて製造番号に基づく情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0059】

請求項17記載の発明は、請求項1ないし13のいずれかに記載の符号生成装置において、秘密入力情報を入力する秘密情報入力手段と、日付情報を取得する日付情報取得手段と、装置の製造番号を認識する製造番号認識手段と、を具備し、前記ハッシュ変換手段は、量子化係数に加えて、前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報に基づいてハッシュ変換を行なう。

#### 【0060】

したがって、各ブロックの量子化係数に加えて、秘密情報、日付情報、製造番

号に基づく情報のうち二つ以上の情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0061】

請求項18記載の発明は、請求項17記載の符号生成装置において、前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報を選択する選択手段を具備し、前記ハッシュ変換手段は、選択した前記情報に基づいてハッシュ変換を行なう。

#### 【0062】

したがって、例えば、ユーザ等が選択した任意の情報をハッシュ変換の種とすることができ、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0063】

請求項19記載の発明は、請求項1ないし18のいずれかに記載の符号生成装置において、対象画像を光学的に読み取った画像を入力する画像入力手段を具備し、前記量子化手段は、前記画像入力手段が入力した画像を量子化する。

#### 【0064】

したがって、例えば、デジタルカメラやスキャナ等の入力手段を用いて入力した画像に電子透かしを埋め込むことができる。

#### 【0065】

請求項20記載の発明の画像処理装置は、請求項1ないし19のいずれかに記載の符号生成装置の符号化手段が生成した符号列データを復号化して量子化係数を生成する復号化手段と、前記量子化係数をブロック単位に分割する復号ブロック分割手段と、前記各ブロックの量子化係数に基づいてハッシュ変換を行ないブロック毎に復号化ハッシュ値を取得する復号ハッシュ変換手段と、前記各ブロックの量子化係数をビットプレーン単位に分割する復号ビットプレーン分割手段と、 $n_i$ 番目の前記ブロックの $m_j$ 番目のビットプレーンの $N$  ( $N$ は偶数)個の有意ビット $Q_{n_i m_j}(x, y)$  ( $x=0, 1, \dots; y=0, 1, \dots$ )によって形成される情報と自然数 $T$ との関係が(7)式を満足するON状態および(8)式を満足するOFF状態によって表わされる偶奇性と、 $n_i$ 番目の前記ブロック

における符号化ハッシュ値の偶奇性と、が一致するか否かを判断する流用検出手段と、を具備する。

【0066】

【数23】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| > \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| \quad \dots (7)$$

【0067】

【数24】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| < \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| \quad \dots (8)$$

【0068】

したがって、請求項1ないし19のいずれかに記載の符号生成装置が生成した符号列データを流用した画像であることを検出することができる。

【0069】

請求項21記載の発明は、請求項20記載の発明の画像処理装置において、前記量子化係数を離散ウェーブレット変換して画像データを生成する画像生成手段と、偶奇性が一致した前記ブロック位置を記憶する流用位置記憶手段と、前記画像データに基づく画像を、記憶した前記ブロック位置を強調して表示部に表示させる強調表示手段と、を具備する。

【0070】

したがって、流用された画像である場合、流用された画像であることを流用されたブロック単位で視認させることができる。

【0071】

請求項22記載の発明は、請求項21記載の画像処理装置において、前記強調表示手段は、記憶した前記ブロック位置を単色で表示させる。

【0072】

したがって、流用された画像である場合、実用上、容易に流用されたブロック



を視覚させることができる。

【0073】

請求項23記載の発明は、請求項21記載の画像処理装置において、前記強調表示手段は、記憶した前記ブロック位置を反転表示させる。

【0074】

したがって、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

【0075】

請求項24記載の発明の符号生成プログラムは、コンピュータにインストールされ、このコンピュータに、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化機能と、前記量子化係数をブロック単位に分割するブロック分割機能と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換機能と、前記各ブロックをビットプレーン単位に分割するビットプレーン分割機能と、n番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n番目の前記ブロックのm番目のビットプレーンのN（Nは偶数）個の有意ビット $Q_{nm}(x, y)$ （ $x=0, 1, \dots$ ;  $y=0, 1, \dots$ ）によって形成される情報と自然数Tとの関係が、（1）式で表わされるON状態または（2）式で表わされるOFF状態を満足するように前記有意ビットのON/OFFを調整する電子透かし埋め込み機能と、ON/OFFを調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化機能と、を実行させる。

【0076】

【数25】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| > T \quad \dots (1)$$

【0077】

【数 26】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| > T \quad \dots (2)$$

【0078】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、単一のビットプレーン内の有意ビットに対してON/OFF調整するため、符号化に際してビットプレーン単位の切り捨てがあった場合にも、有意ビットのON/OFFによって埋め込まれる電子透かしを消滅させることはない。さらに、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項42記載の発明の画像処理プログラムを実行することにより、画像の流用をブロック単位で検出することができる。

【0079】

請求項25記載の発明の符号生成プログラムは、コンピュータにインストールされ、このコンピュータに、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化機能と、前記量子化係数をブロック単位に分割するブロック分割機能と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換機能と、前記各ブロックをビットプレーン単位に分割するビットプレーン分割機能と、n番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、n番目の前記ブロックのm<sub>j</sub>番目のビットプレーンのN（Nは偶数）個の有意ビットQ<sub>n m<sub>j</sub></sub>（x, y）（x=0, 1, …; y=0, 1, …）によって形成される情報と自然数Tとの関係が、（3）式で表わされるON状態または（4）式で表わされるOFF状態を満足するように前記有意ビットのON/OFFを調整する電子透かし埋め込み機能と、ON/OFFを調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化機能と

、を実行させる。

【0080】

【数27】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| > T$$

... (3)

【0081】

【数28】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(ik, ik) \right| > T$$

... (4)

【0082】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項42記載の発明の画像処理プログラムを実行することにより、画像の流用をブロック単位で検出することができる。さらに、ON/OFF調整する有意ビットを複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を抑制するとともに、流用の検出に際しての対象領域の分解能を上げることができる。

【0083】

請求項26記載の発明の符号生成プログラムは、コンピュータにインストールされ、このコンピュータに、画像を複数に分割したタイル毎に画素値を離散ウェーブレット変換して量子化した量子化係数を生成する量子化機能と、前記量子化係数をブロック単位に分割するブロック分割機能と、前記各ブロックの前記量子化係数に基づいてハッシュ変換を行ない前記ブロック毎に符号化ハッシュ値を取得するハッシュ変換機能と、前記各ブロックをビットプレーン単位に分割するビ

ットプレーン分割機能と、 $n_i$  番目の前記ブロックにおける符号化ハッシュ値の偶奇性に応じて、 $n_i$  番目の前記ブロックの  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x=0, 1, \dots; y=0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(5) 式で表わされる  $ON$  状態または (6) 式で表わされる  $OFF$  状態を満足するように前記有意ビットの  $ON/OFF$  を調整する電子透かし埋め込み機能と、 $ON/OFF$  を調整した前記有意ビットを含む前記量子化係数を符号化して符号列データを生成する符号化機能と、を実行させる。

【0084】

【数29】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i_k, i_k) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i_k, i_k) \right| > T$$

... (5)

【0085】

【数30】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k m_k}(i_k, i_k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k m_k}(i_k, i_k) \right| > T$$

... (6)

【0086】

したがって、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。また、有意ビットの  $ON/OFF$  調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項42記載の発明の画像処理プログラムを実行することにより、画像の流用をブロック単位で検出することができる。さらに、 $ON/OFF$  調整する有意ビットを複数のブロックの複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を効果的に抑制するとともに、流用の検出に際しての対象領域の分解能

をより上げることができる。

#### 【0087】

請求項 27 記載の発明は、請求項 24 ないし 26 のいずれかに記載の符号生成プログラムにおいて、前記電子透かし埋め込み機能は、前記符号化ハッシュ値が偶数である場合に N 個の前記有意ビットによって形成される情報と自然数 T との関係 ON 状態とし前記符号化ハッシュ値が奇数である場合に N 個の前記有意ビットによって形成される情報と自然数 T との関係 OFF 状態とする第 1 の方式、または、前記符号化ハッシュ値が奇数である場合に N 個の前記有意ビットによって形成される情報と自然数 T との関係 ON 状態とし前記符号化ハッシュ値が偶数である場合に N 個の前記有意ビットによって形成される情報と自然数 T との関係 OFF 状態とする第 2 の方式のいずれかの方式により前記有意ビットの ON/OFF を調整する。

#### 【0088】

したがって、第 1 の方式または第 2 の方式の 2 つの方式のうちいずれか一方を選択的に用いることにより、埋め込まれる電子透かしを、効果的に第三者に解読し難くすることができる。

#### 【0089】

請求項 28 記載の発明は、請求項 27 記載の符号生成プログラムにおいて、前記第 1 の方式と前記第 2 の方式とのいずれか一方を切替自在に設定する方式設定機能を前記コンピュータに実行させ、前記電子透かし埋め込み機能は、設定された方式にしたがって偶奇性を合わせる。

#### 【0090】

したがって、第 1 の方式または第 2 の方式を切替自在に設定することができる。

#### 【0091】

請求項 29 記載の発明は、請求項 28 記載の符号生成プログラムにおいて、前記方式設定機能は、前記符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて、前記第 1 の方式または前記第 2 の方式を設定する。

**【0092】**

したがって、符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

**【0093】**

請求項30記載の発明は、請求項28記載の符号生成プログラムにおいて、前記方式設定機能は、前記符号化ハッシュ値と外部から入力された秘密情報とに基づいて、前記第1の方式または前記第2の方式を設定する。

**【0094】**

したがって、秘密情報が入力された場合には、符号化ハッシュ値と秘密情報とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

**【0095】**

請求項31記載の発明は、請求項24ないし30のいずれかに記載の符号生成プログラムにおいて、前記符号化機能は、上位のビットプレーンから下位のビットプレーン方向へ符号化を行ない、OFFビットをONにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをOFFにし、ONビットをOFFにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをONにした符号列データを生成する。

**【0096】**

したがって、ビットプレーンの上位から下位方向への符号化においてビットのON/OFFを均等に行ない、電子透かしを埋め込むことによる画質劣化を抑えることができる。

**【0097】**

請求項32記載の発明は、請求項24ないし31のいずれかに記載の符号生成プログラムにおいて、前記量子化係数を選択的に取得する量子化係数選択機能を前記コンピュータに実行させ、前記電子透かし埋め込み手段は、選択的に取得した前記量子化係数における前記有意ビットのON/OFFを行なう。

**【0098】**

したがって、全ての有意ビットを ON/OFF 調整を行なう場合と比較して電子透かしを埋め込むことによる画質劣化を抑えることができる。

【0099】

請求項 33 記載の発明は、請求項 32 記載の符号生成プログラムにおいて、前記量子化係数選択機能により選択する前記量子化係数は、隣り合う前記量子化係数との差がしきい値以上である前記量子化係数である。

【0100】

したがって、隣り合う量子化係数との差がしきい値以上である、すなわち、隣り合う量子化係数に対して変化の激しい量子化係数における有意ビットを ON/OFF することにより、電子透かしを埋め込むことによる画質劣化をより効果的に抑えることができる。

【0101】

請求項 34 記載の発明は、請求項 33 記載の符号生成プログラムにおいて、前記しきい値は調整可能である。

【0102】

したがって、例えば、画質劣化程度や流用の検出精度等に応じて、使用目的に応じたしきい値を設定することができる。

【0103】

請求項 35 記載の発明は、請求項 33 または 34 記載の符号生成装置において、前記量子化係数に前記しきい値を埋め込むしきい値埋め込み機能を前記コンピュータに実行させ、前記符号化機能は、前記しきい値を埋め込んだ前記量子化係数を符号化した符号列データを生成する。

【0104】

したがって、例えば、画像が流用された場合にも、請求項 42 記載の発明の画像処理プログラムを実行することにより、符号列データ中に埋め込んだしきい値を復元して活用することができる。

【0105】

請求項 36 記載の発明は、請求項 32 ないし 35 のいずれか一に記載の符号生成プログラムにおいて、前記量子化係数選択機能により取得する前記量子化係数

の取得頻度は調整可能である。

【0106】

したがって、例えば、目的とする画質程度等に応じた頻度で量子化係数を取得することにより、電子透かしを埋め込むことによる画質劣化の程度を管理することができる。

【0107】

請求項37記載の発明は、請求項24ないし36のいずれかーに記載の符号生成プログラムにおいて、前記ハッシュ変換機能は、前記量子化係数に加えて、外部から入力された秘密情報に基づいてハッシュ変換を行なう。

【0108】

したがって、各ブロックの量子化係数に加えて外部から入力された秘密情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

【0109】

請求項38記載の発明は、請求項24ないし36のいずれかーに記載の符号生成プログラムにおいて、前記ハッシュ変換機能は、前記量子化係数に加えて、日付情報に基づいてハッシュ変換を行なう。

【0110】

したがって、各ブロックの量子化係数に加えて日付情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

【0111】

請求項39記載の発明は、請求項24ないし36のいずれかーに記載の符号生成プログラムにおいて、前記ハッシュ変換機能は、前記量子化係数に加えて、装置の製造番号に基づく情報に基づいてハッシュ変換を行なう。

【0112】

したがって、各ブロックの量子化係数に加えて製造番号に基づく情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。



## 【0113】

請求項40記載の発明は、請求項24ないし36のいずれかに記載の符号生成プログラムにおいて、前記ハッシュ変換機能は、前記量子化係数に加えて、外部から入力された秘密情報、日付情報、装置の製造番号に基づく情報のうち二つ以上の情報に基づいてハッシュ変換を行なう。

## 【0114】

したがって、各ブロックの量子化係数に加えて、外部から入力された秘密情報、日付情報、製造番号に基づく情報のうち二つ以上の情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

## 【0115】

請求項41記載の発明は、請求項40記載の符号生成プログラムにおいて、前記秘密情報、前記日付情報、前記製造番号に基づく情報のうち二つ以上の情報を選択する選択機能を前記コンピュータに実行させ、前記ハッシュ変換機能は、選択した前記情報に基づいてハッシュ変換を行なう。

## 【0116】

したがって、例えば、ユーザ等が選択した任意の情報をハッシュ変換の種とすることができ、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

## 【0117】

請求項42記載の発明の画像処理プログラムは、コンピュータにインストールされ、このコンピュータに、請求項24ないし41のいずれかに記載の符号生成プログラムの実行により生成した符号列データを復号化して量子化係数を生成する復号化機能と、前記量子化係数をブロック単位に分割する復号ブロック分割機能と、前記各ブロックの量子化係数に基づいてハッシュ変換を行ないブロック毎に復号化ハッシュ値を取得する復号ハッシュ変換機能と、前記各ブロックの量子化係数をビットプレーン単位に分割する復号ビットプレーン分割機能と、 $n_i$ 番目の前記ブロックの $m_j$ 番目のビットプレーンの $N$  ( $N$ は偶数)個の有意ビット $Q_{n_i m_j}(x, y)$  ( $x=0, 1, \dots; y=0, 1, \dots$ )によって形成され

る情報と自然数Tとの関係が(7)式を満足するON状態および(8)式を満足するOFF状態によって表わされる偶奇性と、 $n_i$ 番目の前記ブロックにおける復号化ハッシュ値の偶奇性と、が一致するか否かを判断する流用検出機能と、を実行させる。

【0118】

【数31】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Qn_k m_k(i_k, i_k) \right| > \left| \sum_{k=\frac{1}{2}N+1}^N Qn_k m_k(i_k, i_k) \right| \quad \dots (7)$$

【0119】

【数32】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Qn_k m_k(i_k, i_k) \right| < \left| \sum_{k=\frac{1}{2}N+1}^N Qn_k m_k(i_k, i_k) \right| \quad \dots (8)$$

【0120】

したがって、請求項24ないし41のいずれかーに記載の符号生成装置が生成した符号列データを流用した画像であることを検出することができる。

【0121】

請求項43記載の発明は、請求項42記載の画像処理プログラムにおいて、前記量子化係数を離散ウェーブレット変換して画像データを生成する画像生成機能と、前記画像データに基づく画像を、偶奇性が一致した前記ブロック位置を強調して表示部に表示させる強調表示機能と、を具備する。

【0122】

したがって、流用された画像である場合、流用された画像であることを流用されたブロック単位で視認させることができる。

【0123】

請求項44記載の発明は、請求項43記載の画像処理プログラムにおいて、前記強調表示機能は、偶奇性が一致した前記ブロック位置を単色で表示させる。

【0124】

したがって、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

【0125】

請求項45記載の発明は、請求項43記載の画像処理プログラムにおいて、前記強調表示機能は、偶奇性が一致した前記ブロック位置を反転表示させる。

【0126】

したがって、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

【0127】

請求項46記載の発明の記憶媒体は、請求項24ないし41のいずれかに記載の符号生成プログラムを記憶し、機械読み取り可能である。

【0128】

したがって、請求項24ないし41のいずれかに記載の発明の作用を得ることができる。

【0129】

請求項47記載の発明の記憶媒体は、請求項42ないし45のいずれかに記載の画像処理プログラムを記憶し、機械読み取り可能である。

【0130】

したがって、請求項42ないし45のいずれかに記載の発明の作用を得ることができる。

【0131】

【発明の実施の形態】

最初に、本発明の実施の形態の前提となる J P E G 2 0 0 0 アルゴリズムの概要について説明する。

【0132】

図1は、J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを示す説明図である。図1に示すような J P E G 2 0 0 0 方式の階層符号化アルゴリズム（以降、J P E G 2 0 0 0 アルゴリズム）によって、デジタル画像データを圧縮して符号列データを生成したり（符号化）、符号列データを伸長して画像データ

を生成したり（復号化）することができる。

#### 【0133】

JPEG2000 アルゴリズムが、従来の JPEG アルゴリズムと比較して、最も大きく異なる点の一つは、変換方式である。JPEG アルゴリズムでは離散コサイン変換（DCT：Discrete Cosine Transform）を用いているのに対し、JPEG2000 方式の階層符号化アルゴリズムでは離散ウェーブレット変換（DWT：Discrete Wavelet Transform）を用いている。DWT は、DCT に比べて、高圧縮領域における画質が良いという長所を有し、この点が JPEG の後継アルゴリズムである JPEG2000 で DWT が採用された大きな理由の一つとなっている。

#### 【0134】

また、JPEG2000 アルゴリズムと JPEG アルゴリズムとの大きな相違点は、JPEG2000 アルゴリズムでは、システムの最終段に符号形成を行なうために、画像の圧縮動作時には圧縮データを符号列データとして生成し、伸長動作時には伸長に必要な符号列データの解釈を行なう機能が追加されていることである。

#### 【0135】

JPEG2000 は、符号列データによって様々な便利な機能を実現できるようになっており、例えば、ブロック・ベースでの DWT におけるオクターブ分割に対応した任意の階層（デコンポジションレベル）で、静止画像の圧縮伸長動作を自由に停止させることができるようになる（後述する図3参照）。また、JPEG2000 では、一つのファイルから低解像度画像（縮小画像）を取り出したり、画像の一部（タイリング画像）を取り出したりすることができるようになる。

#### 【0136】

入力／出力される原画像の画像データに対しては、例えば、原色系の R（赤）／G（緑）／B（青）の各コンポーネントからなる RGB 表色系や、補色系の Y（黄）／M（マゼンタ）／C（シアン）の各コンポーネントからなる YMC 表色系から、YUV あるいは YCbCr 表色系への変換又は逆変換が行なわれる。

**【0137】**

カラー画像は、一般に、図2に示すように、原画像の各コンポーネント111が、矩形をした領域によって分割される。この分割された矩形領域は、一般にブロックあるいはタイルと呼ばれているものであるが、J P E G 2 0 0 0では、タイルと呼ぶことが一般的であるため、以下、このような分割された矩形領域をタイル112と記述することにする。

**【0138】**

J P E G 2 0 0 0 アルゴリズムにおける画像データの圧縮伸長プロセスを実行する際には、個々のタイル112が基本単位となり、画像データの圧縮伸長動作は、コンポーネント111毎、また、タイル112毎に、独立に行われる。

**【0139】**

まず、J P E G 2 0 0 0 アルゴリズムにおける画像データの符号化について説明する。J P E G 2 0 0 0 アルゴリズムにおける画像データの符号化に際しては、図1に示すように、各コンポーネント111の各タイル112のデータに対して色空間変換を施した後、2次元ウェーブレット変換（順変換）を施して、周波数帯に空間分割する。

**【0140】**

ここで、図3は、デコンポジションレベル数が3の場合の、各デコンポジションレベルにおけるサブバンドを示している。デコンポジションレベル数（施すウェーブレット変換の数）が3の場合、まず、原画像のタイル分割によって得られたタイル原画像（0LL）（デコンポジションレベル0）に対して、2次元ウェーブレット変換を施し、デコンポジションレベル1に示すサブバンド（1LL，1HL，1LH，1HH）を分離する。そして引き続き、この階層における低周波成分1LLに対して、2次元ウェーブレット変換を施し、デコンポジションレベル2に示すサブバンド（2LL，2HL，2LH，2HH）を分離する。順次同様に、低周波成分2LLに対しても、2次元ウェーブレット変換を施し、デコンポジションレベル3に示すサブバンド（3LL，3HL，3LH，3HH）を分離する。図3では、各デコンポジションレベルにおいて符号化の対象となるサブバンドを、網掛けで表してある。例えば、デコンポジションレベル数を3とし

たとき、網掛けで示したサブバンド（3HL, 3LH, 3HH, 2HL, 2LH, 2HH, 1HL, 1LH, 1HH）が符号化対象となり、3LLサブバンドは符号化されない。

#### 【0141】

次いで、指定した符号化の順番で符号化の対象となるビットが定められ、定められた対象ビット周辺のビットからコンテキストを生成し（量子化）、量子化の処理が終わったウェーブレット係数を、個々のサブバンド毎に、「プレシнкт」と呼ばれる重複しない矩形に分割する。これは、インプリメンテーションでメモリを効率的に使うために導入されたものである。図4に示すように、一つのプレシнктは、空間的に一致した3つの矩形領域からなっている。

#### 【0142】

更に、個々のプレシнктは、重複しない矩形の「コード・ブロック」に分けられる。この「コード・ブロック」は、エントロピー・コーディングを行なう際の基本単位となる。

#### 【0143】

ウェーブレット変換後の係数値は、そのまま量子化し符号化することも可能であるが、JPEG2000では符号化効率を上げるために、係数値を「ビットプレーン」単位に分解し、画素あるいはコード・ブロック毎に「ビットプレーン」に順位付けを行なうことができる。

#### 【0144】

ここで、図5は、ビットプレーンに順位付けする手順の一例を示す説明図である。図5に示すように、この例は、原画像（32×32画素）を16×16画素のタイル4つで分割した場合で、デコンポジションレベル1のプレシнктとコード・ブロックとの大きさを、各々8×8画素と4×4画素としている。プレシнктとコード・ブロックの番号は、ラスタ順に付けられており、この例では、プレシнктが番号0から3まで、コード・ブロックが番号0から3まで割り当てられている。タイル境界外に対する画素拡張にはミラーリング法を使い、可逆（5，3）フィルタでウェーブレット変換を行ない、デコンポジションレベル1のウェーブレット係数値を求めている。

## 【0145】

また、タイル0／プレシント3／コード・ブロック3について、代表的な「レイヤ」構成の概念の一例を示す説明図も図5に併せて示す。変換後のコード・ブロックは、サブバンド（1LL，1HL，1LH，1HH）に分割され、各サブバンドにはウェーブレット係数値が割り当てられている。

## 【0146】

レイヤの構造は、ウェーブレット係数値を横方向（ビットプレーン方向）から見ると理解し易い。1つのレイヤは任意の数のビットプレーンから構成される。この例では、レイヤ0，1，2，3は、各々、1，3，1，3のビットプレーンから成っている。そして、LSB（Least Significant Bit：最下位ビット）に近いビットプレーンを含むレイヤ程、先に量子化の対象となり、逆に、MSB（Most Significant Bit：最上位ビット）に近いレイヤは最後まで量子化されずに残ることになる。LSBに近いレイヤから破棄する方法はトランケーションと呼ばれ、量子化率を細かく制御することが可能である。

## 【0147】

続いて、コンテキストと対象ビットとから確率推定によって、各コンポーネントのタイルに対する符号化を行なう。これにより、原画像の全てのコンポーネントについて、タイル単位で符号化処理が行われる。

## 【0148】

最後に、全符号列データを1本の符号列データに結合するとともに、それにタグを付加する処理を行なう。

## 【0149】

次に、JPEG2000アルゴリズムにおける画像データの復号化について説明する。符号列データの復号化に際しては、画像データの符号化時とは逆に、各コンポーネントの各タイルの符号列データから画像データを生成する。この場合、外部より入力した符号列データに付加されたタグ情報を解釈し、符号列データを各コンポーネントの各タイルの符号列データに分解し、その各コンポーネントの各タイルの符号列データ毎に復号化処理（伸長処理）を行なう。このとき、符号列データ内のタグ情報に基づく順番で復号化の対象となるビットの位置が定め

られるとともに、定められた対象ビット位置の周辺ビット（既に復号化を終えている）の並びからコンテキストを生成し、このコンテキストと符号列データとから確率推定によって復号化を行なって対象ビットを生成し、それを対象ビットの位置に書き込む。

#### 【0150】

このようにして復号化したデータは、周波数帯域毎に空間分割されているため、この画像データに対して2次元ウェーブレット変換（逆変換）を行なうことにより、画像データの各コンポーネント111の各タイル112を復元し、復元したデータに対して色空間逆変換を行なうことで元の表色系の画像データに変換する。

#### 【0151】

以上が、J P E G 2 0 0 0 アルゴリズムの概要である。

#### 【0152】

画像データの符号化に際しては、入力された画像データをウェーブレット変換した結果の係数を量子化するまでは、可逆または非可逆な変換過程をとることができる。量子化の処理が終わったウェーブレット係数からエントロピー符号化等の符号列データを生成するまでは可逆変換過程となる。また、画像データの復号化に際して、入力された（圧縮保存済みの）符号列データからウェーブレット係数データ（または、量子化係数データ：可逆圧縮の場合は量子化しないため）を復号化するまでは、可逆変換過程となり、復号化したウェーブレット係数データから画像データを生成するまでは可逆または非可逆な変換過程をとることができる。

#### 【0153】

以下に、本発明の第1の実施の形態について図6ないし図10を参照して説明する。本発明では、上述したJ P E G 2 0 0 0 アルゴリズムにおける量子化係数を使用して、J P E G 2 0 0 0 圧縮処理内で、量子化係数に電子透かしを埋め込むとともに、電子透かしが埋め込まれた量子化係数を解読の可否により画像の流用の有無を検出する符号生成装置および画像処理装置としての画像管理装置への適用例を示す。



## 【0154】

図6は、本実施の形態の画像管理装置の構成を概略的に説明するブロック図である。図6中では、ハード構成とマイクロコンピュータによるソフト処理等の機能とが混在して示されている。

## 【0155】

本実施の形態の画像管理装置1は、全体制御部2、画像撮影部3、操作入力部4、表示部5、外部記憶装置6、メモリ7、非可逆圧縮部8、電子透かし埋め込み部9、H a s h変換部10、可逆圧縮部11、画像再生部12、可逆伸長部13、電子透かし解読部14、非可逆伸長部15、および、流用表示制御部16等をバスライン17などによって接続することにより構成されている。

## 【0156】

全体制御部2は、画像管理装置1全体の動作及び機能を制御する図示しないマイクロコンピュータを主体として構成されている。マイクロコンピュータは、画像管理装置1が備える各部を駆動制御するCPUや、CPUが実行する各種制御プログラムを格納するROM、可変的なデータを書き換え自在に記憶するとともにCPUのワークエリアとして機能するRAM等（いずれも図示せず）を接続することによって構成されており、一般的には、CPUのみを代表として、単に「CPU」と略称されることもある。マイクロコンピュータ（CPU）は、計時機能を有しており、後述する電子透かしの埋め込みに際しては、この計時機能により日付情報を取得することができる。ここに、日付情報取得手段としての機能が実現される。

## 【0157】

ROMには、全体制御部2が実行する各種制御プログラムが格納されており、画像撮影部3、操作入力部4、表示部5、外部記憶装置6、メモリ7、非可逆圧縮部8、電子透かし埋め込み部9、H a s h変換部10、可逆圧縮部11、画像再生部12、可逆伸長部13、電子透かし解読部14、非可逆伸長部15、および、改ざん表示制御部16が実現する各機能は、全体制御部2が各種制御プログラムを実行することによって実現することができる。

## 【0158】

画像撮影部 3 は、セットされた写真や帳票等をスキャンすることで画像を読み取ってイメージ画像データを入力し、画像入力手段として機能する。公知の技術であるため図示および説明を省略するが、画像撮影部 3 は、例えば、スキャン光学系及び CCD などのイメージセンサとその駆動回路等を有するイメージスキャナやデジタルカメラ等によって実現することができる。

#### 【0159】

操作入力部 4 は、ユーザとの間におけるインターフェイスとして機能し、ユーザによって操作されることにより、各種入力信号を全体制御部 2 に出力する。全体制御部 2 は、操作入力部 4 からの出力信号に応じて、各種操作指示や機能選択指令を発行したり、編集データ等を入力したりする。公知の技術であるため図示および説明を省略するが、操作入力部 4 としては、例えば、キーボードやマウス、あるいは、タッチパネル等を用いることができる。本実施の形態では、操作入力部 4 が操作されることによって、後述するように電子透かしデータが埋め込まれた画像データの乱数化を開始したり、乱数化された画像データ中に埋め込まれた電子透かしの解読に際して必要情報を入力したりすることができる。

#### 【0160】

表示部 5 は、画像撮影部 3 が入力したイメージ画像データに基づく画像や、操作ガイダンス等を表示する。本実施の形態の表示部 5 は、表示面上に配列された、R (Red) ・ G (Green) ・ B (Blue) の各色の図示しない入力端子を備えており、各色の入力端子に入力する信号を調整して各色の入力端子の明るさを変えることで、表示部 5 に配列された RGB の各色の入力端子の明るさを最大にした白色から、表示部 5 に配列された RGB の各色の入力端子の明るさを最小にした黒色までを段階的に合成することが可能である。表示部 5 における表示状態は、操作入力部 4 が操作されることにより、ユーザの所望の表示状態に変更することができる。表示部 5 における表示状態として、例えば、電子透かし解読結果を入力イメージ画像データと重ね合わせて表示させたり、どちらか一方のみを選択して表示させたりすることができる。

#### 【0161】

外部記憶装置 6 は、画像撮影部 3 で撮影した画像データや全体制御部 2 で実行

する各種プログラムを、CD-ROM等の可搬性を有するメディア18に記憶させるとともに、可搬性を有するメディア18に記憶されたプログラムを読み取る。外部記憶装置6は、例えば、電子透かし埋め込み部9や可逆圧縮部11での処理によって電子透かしが埋め込まれた圧縮データ、電子透かし解読部14によって改ざんを検出した画像領域部のデータ等をメディア18に記憶させる。

#### 【0162】

ところで、本実施の形態の外部記憶装置6は、可搬性を有するメディア18に記憶された、符号生成プログラムや画像処理プログラムを読み取ることが可能である。符号生成プログラムや画像処理プログラムは、実行することにより後述する電子透かしの埋め込みや電子透かしの検出を行なうプログラムであり、本実施の形態では、可搬性を有するメディア18によって記憶媒体が実現されている。

#### 【0163】

なお、本実施の形態では、可搬性を有するメディア18によって記憶媒体を実現するようにしたが、これに限るものではなく、符号生成プログラムや画像処理プログラムを記憶するフレキシブルディスク（FD）や光磁気ディスク（OMD）等の可搬性を有するメディアによって記憶媒体を実現するようにしてもよい。可搬性を有するメディア18に記憶された符号生成プログラムや画像処理プログラムは、外部記憶装置6によって読み取る（または、インストールする）ことにより、RAMに記憶され、全体制御部2がRAMに記憶された符号生成プログラムや画像処理プログラムを実行して、後述する電子透かしの埋め込みや電子透かしの検出を行なうことが可能であるため、メディア18から符号生成プログラムや画像処理プログラムがインストールされたRAMによっても記憶媒体を実現することができる。

#### 【0164】

また、符号生成プログラムや画像処理プログラムは、可搬性を有する各種メディア（または、RAM）に記憶されているものに限るものではなく、例えば、インターネット等を介して、画像管理装置1以外の外部装置からダウンロードしたものであってもよい。

#### 【0165】

メモリ 7 は、画像撮影部 3 によって読み取ったイメージ画像データや、図 1 に示す J P E G 2 0 0 0 アルゴリズム内で生成される各種データ等を格納する大容量のメモリである。メモリ 7 は、例えば、R A M あるいはハードディスク等によって実現することができる。図 1 に示す J P E G 2 0 0 0 アルゴリズム内で生成されるデータとしては、電子透かしが埋め込まれて J P E G 2 0 0 0 圧縮された後に一旦保存された符号列データ、画像再生部 1 2 によって再生されてた電子透かしが埋め込まれた画像データ、及び、可逆伸長部 1 3 から非可逆伸長部 1 5 における処理で伸長された画像データ等がある。また、メモリ 7 には、画像管理装置 1 の製造番号や、後述する電子透かしの埋め込みに際して画像管理装置 1 の外部から入力された秘密情報等を記憶するエリアが確保されている。これにより、後述する電子透かしの埋め込みに際して、エリアに記憶された画像管理装置 1 の製造番号に基づく情報を種とした H a s h 変換を行なうことができ、ここに、製造番号認識手段が実現される。

#### 【0166】

非可逆圧縮部 8 は、画像撮影部 3 で読み取って外部記憶装置 6 やメモリ 7 に格納されている画像データを使用して、デジタル画像データを非可逆に変換圧縮する処理を施して、量子化係数を生成する。すなわち、非可逆圧縮部 8 は、図 1 中に示す A 処理を行なう。非可逆圧縮部 8 が生成した量子化係数は、メモリ 7 に格納される。

#### 【0167】

電子透かし埋め込み部 9 は、非可逆圧縮部 8 で変換され、メモリ 7 に格納されている量子化係数を使用して、上述したような J P E G 2 0 0 0 圧縮処理内で、量子化係数に電子透かしの埋め込む処理を施す。詳細は後述するが、電子透かし埋め込み部 9 は、図 1 中 A 処理と B 処理との間に相当する箇所で電子透かしの埋め込む処理を行ない、埋め込む電子透かしとして、ハッシュ (H a s h) 変換部で乱数化した (H a s h 変換した) データを用いる。

#### 【0168】

H a s h 変換部 1 0 は、電子透かし埋め込み部 9 で透かし情報を埋め込む際に、J P E G 2 0 0 0 処理内の量子化係数に対して、ハッシュ (H a s h) 関数に

基づくハッシュ (H a s h) 変換を施して乱数化する。

【0169】

本実施の形態では、元のデータが解読できないようにランダムイズすることを「乱数化」とし、この乱数化の機能に、元のデータを復元することができる機能を加えた機能である暗号化と区別して説明する。

【0170】

ここで、H a s h関数とは、引数を種 (タネ) にして生成する一方向性の乱数発生関数であり、以下に示す性質を持っている (出典：電子情報通信学会誌 2000年2月 “公平性保証とプライバシー保護” 佐古和恵)。

性質1：出力値から入力値は推測できない。

性質2：入力値が1 b i tでも変ると、出力値は全面的に変化する。

性質3：同じ出力になる異なる二つの入力の探索は現実的に不可能。

【0171】

H a s h変換は、生成後のデータから元のデータを推定することが不可能であるため、電子透かしの埋め込みに際してH a s h変換を用いることにより、流用を確実に検出することができる。

【0172】

可逆圧縮部11は、図1中に示すB処理を行ない、電子透かし埋め込み部9によって電子透かしが埋め込まれた量子化係数に対して可逆変換を施すことにより、電子透かしが埋め込まれた量子化係数を劣化させることなく圧縮する。可逆圧縮部11で圧縮されたデータは、外部記憶装置6やメモリ7などに保存される。

【0173】

画像再生部12は、外部記憶装置6やメモリ7などに保存されている電子透かしが埋め込まれたJ P E G 2 0 0 0圧縮データを読み取るための制御を行なう。

【0174】

可逆伸長部13は、図1中に示すC処理を行ない、画像再生部12で読み取られたJ P E G 2 0 0 0圧縮データを使用して、可逆圧縮部11の変換処理に対応する逆変換を行なうことによって量子化係数を可逆的に復元する。可逆伸長部13で伸長した量子化係数は、メモリ7に格納される。

## 【0175】

電子透かし解読部14は、図1中C処理とD処理との間に相当する箇所で、可逆伸長部13によって復元されてメモリ7に格納されている量子化係数を使用して、電子透かしが埋め込まれた画像データの中の電子透かしが解読可能かどうかで、画像の流用の有無を判断する。詳細は後述するが、電子透かし解読部14は、メモリ7に格納されている量子化係数をH a s h変換部で乱数化して埋め込まれた電子透かしを解読する。電子透かし解読部14において電子透かしが解読できない場合、解読できないブロック位置をメモリ7に記憶する。

## 【0176】

上述したH a s h変換部10は、電子透かし解読部14における暗号の解読に際して、図1に示すJ P E G 2 0 0 0処理内の量子化係数に対してH a s h変換を施して乱数化する。

## 【0177】

非可逆伸長部15は、図1中に示すD処理を行ない、電子透かし解読部14による流用の有無の検出結果に基づいて、非可逆圧縮部8の変換処理に対応する逆変換を行なうことにより画像を復元する。

## 【0178】

流用表示制御部16は、後述する流用画像の検出に際して、電子透かしが解読できないブロックがある場合、復元した画像データとメモリ7に記憶されたブロック位置情報とに基づいて、記憶したブロック位置の画像が黒色で塗り潰されて表示されるような画像データを展開する。

## 【0179】

次に、電子透かしの埋め込みに際して画像管理装置1が行なう動作について図7を参照して説明する。本実施の形態では、符号生成プログラムの実行により電子透かしの埋め込みが行われる。図7の処理は、画像撮影部3による画像撮影時に実行される。画像撮影部3による画像撮影に先立って、ユーザは、操作入力部4において入力秘密キーを操作することにより秘密情報を入力する。ここに、秘密情報入力手段としての機能が実現される。秘密情報としては、例えば、ユーザが任意に設定可能であって英数字によって構成される複数桁の暗証番号等がある

。

#### 【0180】

電子透かしの埋め込みに際しては、まず、操作入力部 4 における入力秘密キーの操作により入力された入力情報をメモリ 7 に保存し（ステップ S 1）、撮影された被写体の画像を多値画像で読み取りメモリ 7 に記憶する（S 2）。

#### 【0181】

続いて、メモリ 7 に記憶された多値画像に色変換を施し、非可逆圧縮部 8 によって、ウェーブレット変換を施して量子化する（S 3）。本実施の形態では、ステップ S 3 における処理を「J P E G 2 0 0 0（図 7 中、J P 2 と記載）圧縮プロセス 1」とし、この J P E G 2 0 0 0 圧縮プロセス 1 によって量子化手段および量子化機能が実現される。

#### 【0182】

次に、J P E G 2 0 0 0 圧縮プロセス 1 で量子化された量子化係数を  $n \times n$  の大きさのブロック B L に分割する（S 4）。ここに、ブロック分割手段およびブロック分割機能が実現される。このとき、隣り合うブロック B L 同士は、図 8（a）に示すようにそれぞれ独立に分離していてもよいし、図 8（b）に示すようにそれぞれの一部を重ねあわせられていてもよい。また、このとき、ステップ S 3 での量子化の際のタイルと同じ大きさにブロック分割しても、異なる大きさにブロック分割してもよい。

#### 【0183】

続いて、分割したブロックにおける量子化係数に対する処理において乱数を発生させる種となるデータ（シードデータ）を初期化する（S 5）。このように、シードデータを初期化することにより、後述する改ざん検出に際して、改ざんが検出された場合に、該改ざん場所をブロック単位で特定することができる。

#### 【0184】

さらに、メモリ 7 を参照して、メモリ 7 に記憶されている入力情報（秘密情報）、画像管理装置 1 の製造番号に基づく情報、あるいは、マイクロコンピュータの計時機能によって取得される日付情報等に基づいて新しい H a s h 値（符号化ハッシュ値）を取得する（S 6）。ここに、ハッシュ変換手段およびハッシュ変

換機能が実現される。

#### 【0185】

なお、ステップS6で取得するH a s h値は、入力情報、画像管理装置1の製造番号に限るものではなく、既に取得したH a s h値やステップS3で生成した量子化係数を用いてもよい。また、ステップS6で取得する符号化H a s h値は、メモリに記憶されている入力情報、画像管理装置1の製造番号に基づく情報、日付情報、既に取得したH a s h値やステップS3で生成した量子化係数等を単独で使用してもよいし、複数を組み合わせて使用してもよい。流用を検出するためにはより多くのデータを用いてH a s h値を取得する方がよい。

#### 【0186】

本実施の形態では、符号化H a s h変換に際して、量子化係数に加えて、入力情報（秘密情報）、画像管理装置1の製造番号、日付等をH a s h変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0187】

このとき、入力情報（秘密情報）、画像管理装置1の製造番号、日付、既に取得した符号化H a s h値やステップS3で生成した量子化係数等の各種情報から、例えば、操作入力部4の操作によって任意の情報を選択し、処理対象となる量子化係数に加えて、選択した任意の情報を種としてH a s h変換を行なうようにしてもよい。ここに、選択手段および選択機能が実現される。H a s h変換の種となる引数を選択可能とすることにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0188】

そして、隣り合うブロックB Lと重なっていない位置であるか否かを判断することにより変更可能領域であるか否かを判断する（S7）。ステップS7では、例えば、図8（a）に示すようにそれぞれ独立に分離したブロックB Lに分割されている場合、分割された隣り合う全てのブロックB L同士が重ならないので、太線で囲まれた範囲、すなわち、全てが変更可能領域B L'であると判断し、図8（b）に示すようにそれぞれの一部を重ねあわせてブロック分割されている場



合、太線で囲む範囲内を変更可能領域  $BL'$  であると判断する。

### 【0189】

変更可能領域  $BL'$  であると判断した場合には (S7 の Y)、 $n$  番目のブロック  $BL$  における符号化 Hash 値の偶奇性に応じて、 $n$  番目のブロックの  $m$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が、(1) 式で表わされる ON 状態または (2) 式で表わされる OFF 状態を満足するように前記有意ビットの ON/OFF を調整して、電子透かしを埋め込む (S8)。ここに、電子透かし埋め込み手段および電子透かし埋め込み機能が実現される。

### 【0190】

#### 【数33】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| > T \quad \dots (1)$$

### 【0191】

#### 【数34】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm}(ik, ik) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm}(ik, ik) \right| > T \quad \dots (2)$$

### 【0192】

ここで、「有意である」状態とは、ビット表現した処理対象となる量子化係数を上位ビットから下位ビット方向に符号化する場合に、注目する係数値が 0 でないことが解っている状態をいい、1 であるビットを既に符号化済みであることをいう。これに対し、「有意でない」状態とは、注目する係数値が 0 であるまたは 0 である可能性がある状態をいい、1 であるビットをまた符号化していない状態をいう。

## 【0193】

また、「ある自然数 $T$ 」は、目的とする電子透かしの耐性強度に応じて任意に設定される値であり、この自然数 $T$ が大きい値である程、埋め込んだ電子透かしの耐性が強くなる。自然数 $T$ は、大きくする程、画像データに対する修飾や改ざん等の画質を劣化させる操作に対する電子透かしの耐性を強くすることができるが、電子透かしを埋め込む以前の元画像データと比較して画質が劣化する。一方で、自然数 $T$ は、小さくする程、画像データに対する修飾や改ざん等の画質を劣化させる操作に対する耐性が弱くなるが、電子透かしを埋め込む以前の元画像データと比較して画質が劣化し難くなる。このため、自然数 $T$ は、電子透かしを埋め込むことによる画質劣化が目立つ大きさよりも僅かに小さい値に設定することが好ましい。また、自然数 $T$ は、例えば、目的とする画質に応じてユーザが任意に設定することも可能である。

## 【0194】

本実施の形態では、ステップS8において、4個の有意ビット $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$ を使用して一組のビット情報を形成し、ステップS6で取得したHash値が奇数である場合に4個の有意ビット $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$ で形成される情報と自然数 $T$ との関係が(9)式を満足するON状態となり、ステップS6で取得したHash値が偶数である場合に4個の有意ビット $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$ で形成される情報と自然数 $T$ との関係が(10)式を満足するOFF状態となるように、有意ビットのON/OFFを行なう。すなわち、Hash値の偶奇性に応じて、4個の有意ビット $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$ と、ある自然数 $T$ との関係が、(9)式または(10)式に示す関係を満たすまで、A, Bに示す以下の処理を繰り返す。

## 【0195】

## 【数 3 5】

$$| Q_{nm}(i1, j1) + Q_{nm}(i2, j2) | - | Q_{nm}(i3, j3) + Q_{nm}(i4, j4) | > T$$

... (9)

```

{
  if( 0 ≤ Qnm (i3, j3) + Qnm (i4, j4))
  then
  {
    if( 2 ≤ Qnm (i3, j3) + Qnm (i4, j4))
    {
      Qnm (i3, j3) = Qnm (i3, j3) - 1 ;
      Qnm (i4, j4) = Qnm (i4, j4) - 1 ;
    }
  }
  else
  {
    if( Qnm (i3, j3) + Qnm (i4, j4) ≤ - 2 )
    {
      Qnm (i3, j3) = Qnm (i3, j3) + 1 ;
      Qnm (i4, j4) = Qnm (i4, j4) + 1 ;
    }
  }

  if( 0 ≤ Qnm (i1, j1) + Qnm (i2, j2))
  then
  {
    Qnm (i1, j1) = Qnm (i1, j1) + 1 ;
    Qnm (i2, j2) = Qnm (i2, j2) + 1 ;
  }
  else
  {
    Qnm (i1, j1) = Qnm (i1, j1) - 1 ;
    Qnm (i2, j2) = Qnm (i2, j2) - 1 ;
  }
}

```

【 0 1 9 6 】

## 【数 3 6】

$$|Q_{nm}(i3, j3) + Q_{nm}(i4, j4)| - |Q_{nm}(i1, j1) + Q_{nm}(i2, j2)| > T$$

... (10)

```

{
  if(0 ≤ Qnm(i3, j3) + Qnm(i4, j4))
  then
  {
    Qnm(i3, j3) = Qnm(i3, j3) + 1;
    Qnm(i4, j4) = Qnm(i4, j4) + 1;
  }
  else
  {
    Qnm(i3, j3) = Qnm(i3, j3) - 1;
    Qnm(i4, j4) = Qnm(i4, j4) - 1;
  }

  if(0 ≤ Qnm(i1, j1) + Qnm(i2, j2))
  then
  {
    if(2 ≤ Qnm(i1, j1) + Qnm(i2, j2))
    {
      Qnm(i1, j1) = Qnm(i1, j1) - 1;
      Qnm(i2, j2) = Qnm(i2, j2) - 1;
    }
  }
  else
  {
    if(Qnm(i1, j1) + Qnm(i2, j2) ≤ -2)
    {
      Qnm(i1, j1) = Qnm(i1, j1) + 1;
      Qnm(i2, j2) = Qnm(i2, j2) + 1;
    }
  }
}

```

## 【0 1 9 7】

このとき、上位のビットプレーンから下位のビットプレーン方向へ符号化を行ない、OFFビットをONにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをOFFにし、ONビットをOFFにする場合は処理対象となるビットプレーンの下位ビットプレーン内の該当する全てのビットをONにする。

## 【0 1 9 8】

これにより、ビットプレーンの上位から下位方向への符号化においてビットのON/OFFを均等に行ない、電子透かしを埋め込むことによる画質劣化を抑え

ることができる。

【0199】

例えば、4個の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  がそれぞれ 0, 1, 0, 0 であり自然数  $T$  が 3 であって、ステップ S6 で取得した Hash 値が奇数である場合、有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  と、ある自然数  $T$  との関係が、(9) 式に示す関係を満たすように (9) 式以下に示す処理を行なう。これにより、電子透かし埋め込み後の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  はそれぞれ 2, 3, 0, 0 となる。

【0200】

また、一旦電子透かし埋め込んだ有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  がそれぞれ 2, 3, 0, 0 であり自然数  $T$  が 3 であって、ステップ S6 で取得した Hash 値が偶数である場合、有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  と、ある自然数  $T$  との関係が、(10) 式に示す関係を満たすように (10) 式以下に示す処理を行なう。これにより、電子透かし埋め込み後の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  はそれぞれ 0, 1, 3, 3 となる。

【0201】

さらに、電子透かし埋め込んだ有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  がそれぞれ 0, 1, 3, 3 であり自然数  $T$  が 3 であって、ステップ S6 で取得した Hash 値が奇数である場合、有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  と、ある自然数  $T$  との関係が、(9) 式に示す関係を満たすように (9) 式以下に示す処理を行なう。これにより、電子透かし埋め込み後の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  はそれぞれ 3, 4, 0, 0 となる。

。

## 【0202】

以降、何回繰り返して電子透かしを埋め込んだ場合にも、有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  は、それぞれ、3, 4, 0, 0と0, 1, 3, 3とが入れ替わるだけである。

## 【0203】

本実施の形態によれば、4個の有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  と、ある自然数  $T$  との関係が、(9)式または(10)式に示す関係を満たすまで、上述の(9)式以下または(10)式以下に示す処理に代えて、以下に示す処理A, Bを繰り返す場合と比較して、電子透かしを埋め込むことによる画質劣化を抑えることができる。

## 【0204】

【数 3 7】

```
A
{
  if( 0 ≤ Qnm (i3,j3)+Qnm (i4,j4))
  then
  {
    Qnm (i3,j3)=Qnm (i3,j3) - 1;
    Qnm (i4,j4)=Qnm (i4,j4) - 1;
  }
  else
  {
    Qnm (i3,j3)=Qnm (i3,j3) + 1;
    Qnm (i4,j4)=Qnm (i4,j4) + 1;
  }

  if( 0 ≤ Qnm (i1,j1)+Qnm (i2,j2))
  then
  {
    Qnm (i1,j1)=Qnm (i1,j1) + 1;
    Qnm (i2,j2)=Qnm (i2,j2) + 1;
  }
  else
  {
    Qnm (i1,j1)=Qnm (i1,j1) - 1;
    Qnm (i2,j2)=Qnm (i2,j2) - 1;
  }
}
```

【 0 2 0 5】

## 【数 38】

```

B
{
  if(  $0 \leq Q_{nm}(i3, j3) + Q_{nm}(i4, j4)$  )
  then
  {
     $Q_{nm}(i3, j3) = Q_{nm}(i3, j3) + 1$ ;
     $Q_{nm}(i4, j4) = Q_{nm}(i4, j4) + 1$ ;
  }
  else
  {
     $Q_{nm}(i3, j3) = Q_{nm}(i3, j3) - 1$ ;
     $Q_{nm}(i4, j4) = Q_{nm}(i4, j4) - 1$ ;
  }

  if(  $0 \leq Q_{nm}(i1, j1) + Q_{nm}(i2, j2)$  )
  then
  {
     $Q_{nm}(i1, j1) = Q_{nm}(i1, j1) - 1$ ;
     $Q_{nm}(i2, j2) = Q_{nm}(i2, j2) - 1$ ;
  }
  else
  {
     $Q_{nm}(i1, j1) = Q_{nm}(i1, j1) + 1$ ;
     $Q_{nm}(i2, j2) = Q_{nm}(i2, j2) + 1$ ;
  }
}

```

## 【0206】

すなわち、4個の有意ビット  $Q_{nm}(i1, j1)$ 、 $Q_{nm}(i2, j2)$ 、 $Q_{nm}(i3, j3)$ 、 $Q_{nm}(i4, j4)$  がそれぞれ 0, 1, 0, 0 であり自然数  $T$  が 3 であって、ステップ S6 で取得した Hash 値が奇数である場合に、有意ビット  $Q_{nm}(i1, j1)$ 、 $Q_{nm}(i2, j2)$ 、 $Q_{nm}(i3, j3)$ 、 $Q_{nm}(i4, j4)$  と、ある自然数  $T$  との関係が、(9) 式に示す関係を満たすように A の処理を行なうと、電子透かし埋め込み後の有意ビット  $Q_{nm}(i1, j1)$ 、 $Q_{nm}(i2, j2)$ 、 $Q_{nm}(i3, j3)$ 、 $Q_{nm}(i4, j4)$  はそれぞれ 2, 3, 0, 0 となる。

## 【0207】

このように、一旦電子透かしを埋め込んだ有意ビット  $Q_{nm}(i1, j1)$ 、 $Q_{nm}(i2, j2)$ 、 $Q_{nm}(i3, j3)$ 、 $Q_{nm}(i4, j4)$  がそれぞれ 2, 3, 0, 0 であり自然数  $T$  が 3 であって、ステップ S6 で取得した Hash





$j3)$ ,  $Q_{nm}(i4, j4)$  で形成される情報と自然数  $T$  との関係が (9) 式を満足する ON 状態となり、ステップ S6 で取得した Hash 値が偶数である場合に 4 個の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  で形成される情報と自然数  $T$  との関係が (10) 式を満足する OFF 状態となるように、有意ビットの ON/OFF を行なうようにしたが、これに限るものではなく、4 個の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  を使用して一組のビット情報を形成し、ステップ S6 で取得した Hash 値が偶数である場合に 4 個の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  で形成される情報と自然数  $T$  との関係が (9) 式を満足する ON 状態となり、ステップ S6 で取得した Hash 値が奇数である場合に 4 個の有意ビット  $Q_{nm}(i1, j1)$ ,  $Q_{nm}(i2, j2)$ ,  $Q_{nm}(i3, j3)$ ,  $Q_{nm}(i4, j4)$  で形成される情報と自然数  $T$  との関係が (10) 式を満足する OFF 状態となるように、有意ビットの ON/OFF を行なうようにしてもよい。

#### 【0212】

本実施の形態では、ステップ S6 で取得したハッシュ値が偶数である場合に 4 個の有意ビットによって形成される情報と自然数  $T$  との関係を ON 状態としステップ S6 で取得したハッシュ値が偶数である場合に 4 個の有意ビットによって形成される情報と自然数  $T$  との関係を OFF 状態とする第 1 の方式と、ステップ S6 で取得したハッシュ値が偶数である場合に 4 個の有意ビットによって形成される情報と自然数  $T$  との関係を ON 状態としステップ S6 で取得したハッシュ値が偶数である場合に 4 個の有意ビットによって形成される情報と自然数  $T$  との関係を OFF 状態とする第 2 の方式と、のいずれか一方の方式を切替自在に設定することができる。第 1 の方式または第 2 の方式の設定は、画像管理装置 1 の製造時（出荷前）に選択的に切り替えて設定してもよいし、操作入力部 4 の操作によって適宜切り替えることを可能にしてもよい。ここに、方式設定手段および方式設定機能が実現される。

#### 【0213】

また、第1の方式または第2の方式の設定は、例えば、ステップS6で取得したハッシュ値と処理対象となる量子化係数の画像中での座標値とに基づき、ハッシュ値と座標値との積が偶数であるか奇数であるかに応じて、第1の方式または第2の方式のいずれか一方を切替自在に設定するようにしてもよい。このように、ハッシュ値と座標値との積が偶数であるか奇数であるかに応じて、第1の方式または第2の方式のいずれか一方を切替自在に設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0214】

さらに、第1の方式または第2の方式の設定は、例えば、操作入力部4の操作によって数値により構成される秘密情報が入力された場合には、ステップS6で取得したハッシュ値と操作入力部4の操作によって入力された秘密情報とに基づき、ハッシュ値と秘密情報との積が偶数であるか奇数であるかに応じて、第1の方式または第2の方式のいずれか一方を切替自在に設定するようにしてもよい。このように、操作入力部4の操作によって秘密情報が入力された場合には、符号化ハッシュ値と秘密情報とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0215】

第1または第2の方式のいずれにしても、偶奇性を合わせる方式を上述したように設定することにより、電子透かしを複数回重ねて埋め込んだ場合にも、N個（本実施の形態では4個）の有意ビットのそれぞれが、電子透かしを埋め込む前と比較して絶対値でT以上変化してしまうことがなくなり、電子透かしを埋め込むことによる画像劣化を抑えることができる。

#### 【0216】

なお、ステップS7で、注目している量子化係数の位置が変更可能領域から外れていれば（S7のN）、透かし入れの処理は行わず、元の量子化係数のままステップS9に進む。

#### 【0217】

処理対象となる全ての量子化係数に対する電子透かし入れが終了したか否かを

判断し（S9）、処理対象となる全ての量子化係数に対する電子透かし入れが終了していない場合には（S9のN）、ステップS6に進み、次の量子化係数に対してステップS6からステップS8までの処理を行なう。

#### 【0218】

処理対象とするブロックBL内の全ての量子化係数に対する電子透かし入れが終了したと判断した場合には（S9のY）、全てのブロックBLに対して電子透かし入れが終了したか否かを判断する（S10）。

#### 【0219】

全てのブロックBLに対して電子透かし入れが終了したと判断した場合には（S10のY）、可逆圧縮部11によって、電子透かし入れが終了した量子化係数に対して可逆圧縮変換を施して符号列データを生成して（S11）、生成した符号列データを外部記憶装置6またはメモリ7に保存する。なお、本実施の形態では、ステップS11の処理を「JPG2000（図7中、JP2と記載）圧縮プロセス2」とし、このJPG2000圧縮プロセス2によって符号化手段および符号化機能が実現される。これによって、メモリ7または外部記憶装置6には、電子透かしが埋め込まれた符号列データが保存される。

#### 【0220】

なお、本実施の形態では、ステップS6で取得した符号化Hash値が奇数である場合にON状態とし、ステップS6で取得した符号化Hash値が偶数である場合にOFF状態としたが、これに限るものではなく、ブロックBLの符号化Hash値が奇数である場合にOFF状態とし、ステップS6で取得した符号化Hash値が偶数である場合にON状態としてもよく、符号化Hash値の偶奇性に対するON状態／OFF状態の対応関係は、例えば、画像管理装置1の製造時等に設定することができる。

#### 【0221】

次に、電子透かしが埋め込まれた符号列データの流用検出に際して画像管理装置1が行なう動作について図9を参照して説明する。図9の処理は、画像再生部12による画像再生時に実行される。本実施の形態では、画像処理プログラムの実行により画像の流用検出が行われる。画像再生部12による画像再生に先立っ

て、ユーザは、操作入力部 4 を操作することにより入力秘密キーを操作することにより秘密情報を入力する。このときに入力する秘密情報は、解読したいデータの符号化に際して入力した秘密情報である。

#### 【0222】

電子透かしが埋め込まれた符号列データの流用検出に際しては、まず、操作入力部 4 における入力秘密キーの操作により入力された入力情報をメモリ 7 に保存し（ステップ S 2 1）、外部記憶装置 6 またはメモリ 7 に記憶された J P E G 2 0 0 0 圧縮データを画像再生部 1 2 によって再生する（S 2 2）。

#### 【0223】

続いて、画像再生部 1 2 によって再生した多値画像の符号列データに対して色空間逆変換を施し、可逆伸長部 1 3 によって、符号列データを量子化する（S 2 3）。本実施の形態では、ステップ S 2 3 における処理を「J P E G 2 0 0 0（図 9 中、J P 2 と記載）伸長プロセス 1」とし、この J P E G 2 0 0 0 伸長プロセス 1 によって復号化手段および復号化機能が実現される。

#### 【0224】

次に、J P E G 2 0 0 0 伸長プロセス 1 で量子化された量子化係数を  $n \times n$  の大きさのブロック B L に分割する（S 2 4）。ここに、復号ブロック分割手段および復号ブロック分割機能が実現される。このとき、隣り合うブロック B L 同士は、図 8（a）に示すようにそれぞれ独立に分離していてもよいし、図 8（b）に示すようにそれぞれの一部を重ねあわせられていてもよい。また、このとき、ステップ S 2 3 での量子化の際のタイルと同じ大きさにブロック分割しても、異なる大きさにブロック分割してもよい。

#### 【0225】

続いて、分割したブロックにおける量子化係数に対する処理において乱数を発生させる種となるデータ（シードデータ）を初期化する（S 2 5）。このように、シードデータを初期化することにより、元データに対する改ざんが検出された場合に、該改ざん場所をブロック単位で特定することができる。

#### 【0226】

さらに、メモリ 7 を参照して、メモリ 7 に記憶されている入力情報、画像管理

装置 1 の製造番号に基づく情報、日付情報等に基づいて新しい H a s h 値（復号化ハッシュ値）を取得する（S 2 6）。ここに、復号ハッシュ変換手段および復号ハッシュ変換機能が実現される。なお、ステップ S 2 6 で取得する H a s h 値は、入力情報、画像管理装置 1 の製造番号に基づく情報、日付情報に限るものではなく、既に取得した H a s h 値やステップ S 2 3 で生成した量子化係数を用いてもよい。また、ステップ S 6 で取得するハッシュ値は、メモリ 7 に記憶されている入力情報、画像管理装置 1 の製造番号、日付、既に取得した H a s h 値やステップ S 2 3 で生成した量子化係数等を単独で使用してもよいし、複数を使用してもよい。流用を検出するためにはより多くのデータを用いて H a s h 値を取得する方がよい。

#### 【0227】

そして、n 番目のブロック B L における対象とする量子化係数の位置が隣り合うブロック B L と重なっていない位置であるか否かを判断することにより、n 番目のブロック B L における対象とする量子化係数が変更可能領域にあるか否かを判断する（S 2 7）。例えば、図 8（a）に示すようにそれぞれ独立に分離してブロック分割されている場合、分割された隣り合う全てのブロック B L 同士が重ならないので、全てを変更可能領域であると判断し、図 8（b）に示すようにそれぞれの一部を重ねあわせてブロック分割されている場合、太線で囲む範囲内を変更可能領域であると判断する。

#### 【0228】

n 番目のブロック B L における対象とする量子化係数が変更可能領域にあると判断した場合には（S 2 7 の Y）、n 番目のブロック B L の m 番目のビットプレーンの N（N は偶数）個の有意ビット  $Q_{nm}(x, y)$ （ $x = 0, 1, \dots$ ;  $y = 0, 1, \dots$ ）によって形成される情報と自然数 T との関係が（7）式を満足する O N 状態および（8）式を満足する O F F 状態によって表わされる偶奇性と、n 番目のブロックにおける H a s h 値の偶奇性と、が一致するか否かを判断する（S 2 8）。ここに、流用検出手段および流用検出機能が実現される。

#### 【0229】

【数 3 9】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| > \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| \quad \dots (7)$$

【0 2 3 0】

【数 4 0】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| < \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| \quad \dots (8)$$

【0 2 3 1】

本実施の形態では、図 7 において、4 個の有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  を使用し、 $n$  番目のブロック  $BL$  の  $Hash$  値に応じて、 $n$  番目のブロック  $BL$  の  $m$  番目のビットプレーンにおける有意ビットの  $ON/OFF$  を調整したため、ステップ  $S28$  においても、4 個の有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  を使用する。なお、このとき、(5) 式および (6) 式における  $n_1, n_2, n_3, n_4$  は、 $n_1 = n_2 = n_3 = n_4$  となり、 $m_1, m_2, m_3, m_4$  は、 $m_1 = m_2 = m_3 = m_4$  となる。

【0 2 3 2】

ステップ  $S28$  では、ステップ  $S26$  で取得した  $Hash$  値が奇数である場合に 4 個の有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  の関係が (11) 式を満足する  $ON$  状態となり、ステップ  $S26$  で取得した  $Hash$  値が偶数である場合に 4 個の有意ビット  $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$  の関係が (12) 式を満足する  $OFF$  状態となるかを判断する。

$$\begin{aligned} & |Q_{nm}(i_1, j_1) + Q_{nm}(i_2, j_2)| \\ & > |Q_{nm}(i_3, j_3) + Q_{nm}(i_4, j_4)| \quad \dots (11) \\ & |Q_{nm}(i_1, j_1) + Q_{nm}(i_2, j_2)| \end{aligned}$$

$$< | Q_{nm}(i_3, j_3) + Q_{nm}(i_4, j_4) | \quad \dots (12)$$

**【0233】**

4個の有意ビット $Q_{nm}(i_1, j_1)$ ,  $Q_{nm}(i_2, j_2)$ ,  $Q_{nm}(i_3, j_3)$ ,  $Q_{nm}(i_4, j_4)$ の関係が(11)または(12)式を満足すると判断した場合(S28のY)、この画像データは流用されたものであると判断してこのブロック位置をメモリ7に記憶する(S29)。ここに、流用位置記憶手段が実現される。

**【0234】**

ステップS27で、注目している量子化係数の位置が変更可能領域から外れていれば(S27のN)、流用検出の処理は行わず、ステップS30に進む。

**【0235】**

処理対象とするブロック内の全ての量子化係数に対する流用検出が終了したか否かを判断し(S30)、処理対象とするブロック内の全ての量子化係数に対する流用検出が終了していない場合には(S30のN)、ステップS26に進み、次の量子化係数に対して電子ステップS26からステップS29までの処理を行なう。

**【0236】**

なお、本実施の形態では、ステップS28において流用された画像データであると判断した場合に、このブロックBLの他の量子化係数に対しても流用検出を行なうようにしたが、これに限るものではなく、単一のブロックBL内のいずれかの量子化係数に基づいて流用された画像データであると判断した場合、このブロックBL内の他の量子化係数についての流用検出を行わず次のブロックBLについての流用検出に移行するようにしてもよい。これにより、流用検出処理の負担を軽減することができる。

**【0237】**

処理対象とするブロックBL内の全ての量子化係数に対する流用検出が終了したと判断した場合には(S30のY)、全てのブロックBLに対して流用検出が終了したか否かを判断する(S31)。

**【0238】**



全てのブロック B L に対して流用検出が終了したと判断した場合には (S 3 1 の Y)、非可逆伸長部 1 5 によって、流用検出が終了した量子化係数に対して非可逆圧縮変換を施して画像データを生成する (S 3 2)。なお、本実施の形態では、ステップ S 3 2 の処理を「J P E G 2 0 0 0 (図 9 中、J P 2 と記載) 伸長プロセス 2」とし、この J P E G 2 0 0 0 伸長プロセス 2 によって画像生成手段および画像生成機能が実現される。

#### 【0239】

そして、J P E G 2 0 0 0 伸長プロセス 2 で生成した画像データとステップ S 2 9 で記憶した流用ブロック位置とに基づいて、流用ブロック位置が黒色で塗り潰された画像を表示部 5 に表示する (S 3 3)。ここに、強調表示手段および強調表示機能が実行される。

#### 【0240】

ステップ S 3 3 では、表示部 5 に配列された R G B の各色の入力端子のうち、改ざんブロック位置に相当する一の入力端子の明るさを最小にすることで、改ざんブロック位置の画像を黒色で表示する。

#### 【0241】

このように、流用された画像である場合には、流用されたブロック位置を強調して表示部 5 に表示させることにより、流用された部分が不自然な画像として表示されるので、流用の有無と流用された位置とを視覚することができる。また、流用ブロック位置を単色で表示させることにより、実用上、容易な処理で流用箇所を視覚させることができる。

#### 【0242】

なお、本実施の形態では、ステップ S 3 3 において、流用ブロック位置が黒色で塗り潰された画像を表示部 5 に表示させるようにしたが、これに限るものではなく、例えば、流用ブロック位置の表示色が反転された画像や、流用ブロック位置が白色や赤色等単色で塗り潰された画像を表示部 5 に表示させるようにしてもよい。

#### 【0243】

本実施の形態によれば、n 番目のブロックにおけるハッシュ値の偶奇性に応じ

て、単一のブロックの単一のビットプレーンの $N$ （本実施の形態では $N=4$ ）個の有意ビット $Q_{nm}(x, y)$ （ $x=0, 1, \dots; y=0, 1, \dots$ ）によって形成される情報と自然数 $T$ との関係が、（１）式で表わされる $ON$ 状態または（２）式で表わされる $OFF$ 状態を満足するように有意ビットの $ON/OFF$ を調整することにより、電子透かしの埋め込みのための演算が、単一のビットプレーン内で閉じられるので、量子化の後段のエントロピー符号化に際してビットプレーン単位の切り捨てがあった場合にも、埋め込まれた電子透かしを消滅させることがない。また、電子透かしのデータ値がブロック毎に決定されているため、画像が流用された場合にも、画像の流用をブロック単位で検出することができる。

#### 【0244】

また、このような流用検出の機能を予めユーザに通知しておくことにより、良識のあるユーザに対して、画像データの流用の抑止効果を期待することができる。

#### 【0245】

さらに、本実施の形態によれば、量子化係数に電子透かしを埋め込むことにより、画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがない。

#### 【0246】

なお、ブロック分割に際しては、隣り合うブロック $BL$ が一部重なり合う重なり量を調整自在としたり、また、隣り合うブロック $BL$ を一部重なり合うようにしてもしなくても分割するブロック $BL$ の大きさを調整自在としたりすることにより、電子透かしの埋め込みにおける処理量や処理速度等を調整することができる。

#### 【0247】

次に、本発明の第２の実施の形態について説明する。なお、第１の実施の形態と同一部分は同一符号で示し、説明も省略する。以下、同様とする。

#### 【0248】

特に図示しないが、本実施の形態の画像管理装置１は、図７に示すステップＳ８における処理が第１の実施の形態とは異なる。

## 【0249】

本実施の形態の画像管理装置 1 は、図 7 に示すステップ S 8 に相当する処理として、n 番目のブロック B L における H a s h 値の偶奇性に応じて、n 番目のブロック B L の m<sub>j</sub> 番目のビットプレーンの N (N は偶数) 個の有意ビット Q n m<sub>j</sub> (x, y) (x = 0, 1, …; y = 0, 1, …) によって形成される情報と自然数 T との関係が、(3) 式で表わされる O N 状態または (4) 式で表わされる O F F 状態を満足するように有意ビットの O N / O F F を調整する。ここに、電子透かし埋め込み手段および電子透かし埋め込み機能が実現される。

## 【0250】

## 【数 4 1】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(i_k, i_k) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(i_k, i_k) \right| > T \quad \dots (3)$$

## 【0251】

## 【数 4 2】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{nm_k}(i_k, i_k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{nm_k}(i_k, i_k) \right| > T \quad \dots (4)$$

## 【0252】

本実施の形態では、4 個の有意ビット Q n m<sub>1</sub> (i<sub>1</sub>, j<sub>1</sub>), Q n m<sub>2</sub> (i<sub>2</sub>, j<sub>2</sub>), Q n m<sub>3</sub> (i<sub>3</sub>, j<sub>3</sub>), Q n m<sub>4</sub> (i<sub>4</sub>, j<sub>4</sub>) を使用して一組のビット情報を形成し、ステップ S 6 で取得した H a s h 値が奇数である場合に 4 個の有意ビット Q n m<sub>1</sub> (i<sub>1</sub>, j<sub>1</sub>), Q n m<sub>2</sub> (i<sub>2</sub>, j<sub>2</sub>), Q n m<sub>3</sub> (i<sub>3</sub>, j<sub>3</sub>), Q n m<sub>4</sub> (i<sub>4</sub>, j<sub>4</sub>) で形成される情報と自然数 T との関係が (13) 式を満足する O N 状態となり、ステップ S 6 で取得した H a s h 値が偶数である場合に 4 個の有意ビット Q n m<sub>1</sub> (i<sub>1</sub>, j<sub>1</sub>), Q n m<sub>2</sub> (i<sub>2</sub>, j<sub>2</sub>), Q n m<sub>3</sub> (i<sub>3</sub>, j<sub>3</sub>), Q n m<sub>4</sub> (i<sub>4</sub>, j<sub>4</sub>) で形成される情報と

自然数  $T$  との関係が (14) 式を満足する OFF 状態となるように、有意ビットの ON/OFF を行なう。すなわち、4 個の有意ビット  $Q_{nm_1}(i_1, j_1)$ ,  $Q_{nm_2}(i_2, j_2)$ ,  $Q_{nm_3}(i_3, j_3)$ ,  $Q_{nm_4}(i_4, j_4)$  と、ある自然数  $T$  との関係が、(13) 式または (14) 式を満たすまで、以下の処理を繰り返す。

【0253】

【数43】

$$|Q_{nm_1}(i_1, j_1) + Q_{nm_2}(i_2, j_2)| - |Q_{nm_3}(i_3, j_3) + Q_{nm_4}(i_4, j_4)| > T \quad \dots (13)$$

```
{
  if(0 ≤ Qnm3(i3, j3) + Qnm4(i4, j4))
  then
  {
    if(2 ≤ Qnm3(i3, j3) + Qnm4(i4, j4))
    {
      Qnm3(i3, j3) = Qnm3(i3, j3) - 1;
      Qnm4(i4, j4) = Qnm4(i4, j4) - 1;
    }
  }
  else
  {
    if(Qnm3(i3, j3) + Qnm4(i4, j4) ≤ -2)
    {
      Qnm3(i3, j3) = Qnm3(i3, j3) + 1;
      Qnm4(i4, j4) = Qnm4(i4, j4) + 1;
    }
  }

  if(0 ≤ Qnm1(i1, j1) + Qnm2(i2, j2))
  then
  {
    Qnm1(i1, j1) = Qnm1(i1, j1) + 1;
    Qnm2(i2, j2) = Qnm2(i2, j2) + 1;
  }
  else
  {
    Qnm1(i1, j1) = Qnm1(i1, j1) - 1;
    Qnm2(i2, j2) = Qnm2(i2, j2) - 1;
  }
}
```

【0254】

## 【数 4 4】

$$| Q_{nm_3}(i3, j3) + Q_{nm_4}(i4, j4) | - | Q_{nm_1}(i1, j1) + Q_{nm_2}(i2, j2) | > T \quad \dots (14)$$

```

{
  if( 0 ≤ Qnm3(i3, j3) + Qnm4(i4, j4))
  then
  {
    Qnm3(i3, j3) = Qnm3(i3, j3) + 1;
    Qnm4(i4, j4) = Qnm4(i4, j4) + 1;
  }
  else
  {
    Qnm3(i3, j3) = Qnm3(i3, j3) - 1;
    Qnm4(i4, j4) = Qnm4(i4, j4) - 1;
  }

  if( 0 ≤ Qnm1(i1, j1) + Qnm2(i2, j2))
  then
  {
    if( 2 ≤ Qnm1(i1, j1) + Qnm2(i2, j2))
    {
      Qnm1(i1, j1) = Qnm1(i1, j1) - 1;
      Qnm2(i2, j2) = Qnm2(i2, j2) - 1;
    }
  }
  else
  {
    if( Qnm1(i1, j1) + Qnm2(i2, j2) ≤ -2 )
    {
      Qnm1(i1, j1) = Qnm1(i1, j1) + 1;
      Qnm2(i2, j2) = Qnm2(i2, j2) + 1;
    }
  }
}

```

## 【0 2 5 5】

また、本実施の形態の画像管理装置 1 は、図 9 に示すステップ S 2 8 に相当する処理として、 $n$  番目のブロック  $BL$  の  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が (5) 式を満足する  $ON$  状態および (6) 式を満足する  $OFF$  状態によって表わされる偶奇性と、 $n$  番目のブロック  $BL$  における符号化  $Hash$  値の偶奇性と、が一致するか否かを判断する。ここに、流用検出手段および流用検出機能が実現される。

## 【0 2 5 6】

本実施の形態では、図 7 において、4 個の有意ビット  $Q_{nm1}(i1, j1)$  ,  $Q_{nm2}(i2, j2)$  ,  $Q_{nm3}(i3, j3)$  ,  $Q_{nm4}(i4, j4)$  を使用し、 $n$  番目のブロック  $BL$  のハッシュ値に応じて、 $n$  番目のブロック  $BL$  の  $m_j$  番目のビットプレーンにおける有意ビットの ON/OFF を調整したため、ステップ S28 においても、4 個の有意ビット  $Q_{nm1}(i1, j1)$  ,  $Q_{nm2}(i2, j2)$  ,  $Q_{nm3}(i3, j3)$  ,  $Q_{nm4}(i4, j4)$  を使用する。なお、(5) 式および (6) 式における  $n1, n2, n3, n4$  は、 $n1 = n2 = n3 = n4$  となる。

#### 【0257】

ステップ S28 では、ステップ S26 で取得した Hash 値が奇数である場合に 4 個の有意ビット  $Q_{nm1}(i1, j1)$  ,  $Q_{nm2}(i2, j2)$  ,  $Q_{nm3}(i3, j3)$  ,  $Q_{nm4}(i4, j4)$  の関係が (15) 式を満足する ON 状態となり、ステップ S26 で取得した Hash 値が偶数である場合に 4 個の有意ビット  $Q_{nm}(i1, j1)$  ,  $Q_{nm}(i2, j2)$  ,  $Q_{nm}(i3, j3)$  ,  $Q_{nm}(i4, j4)$  の関係が (16) 式を満足する OFF 状態となるかを判断する。

$$\begin{aligned} & |Q_{nm1}(i1, j1) + Q_{nm2}(i2, j2)| \\ & > |Q_{nm3}(i3, j3) + Q_{nm4}(i4, j4)| \quad \dots (15) \end{aligned}$$

$$\begin{aligned} & |Q_{nm1}(i1, j1) + Q_{nm2}(i2, j2)| \\ & < |Q_{nm3}(i3, j3) + Q_{nm4}(i4, j4)| \quad \dots (16) \end{aligned}$$

#### 【0258】

本実施の形態によれば、複数のビットプレーンにまたがって複数個の有意ビットを使用して電子透かしを埋め込むため、画質の劣化を抑えて電子透かしの耐性を強くするとともに、電子透かしを埋め込む場所が分散されるので、流用検出のための調査対象となる領域の分解能を上げることができる。

#### 【0259】

次に、本発明の第 3 の実施の形態について説明する。

#### 【0260】

特に図示しないが、本実施の形態の画像管理装置 1 は、図 7 に示すステップ S

8における処理が第1の実施の形態とは異なる。

### 【0261】

本実施の形態の画像管理装置1は、図7に示すステップS8に相当する処理として、n番目のブロックBLにおけるHash値の偶奇性に応じて、n番目のブロックBLのmj番目のビットプレーンのN（Nは偶数）個の有意ビットQn<sub>i</sub>m<sub>j</sub>（x，y）（x=0，1，…；y=0，1，…）によって形成される情報と自然数Tとの関係が、（5）式で表わされるON状態または（6）式で表わされるOFF状態を満足するように前記有意ビットのON／OFFを調整する。ここに、電子透かし埋め込み手段および電子透かし埋め込み機能が実現される。

### 【0262】

【数45】

$$\left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| - \left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| > T \quad \dots (5)$$

### 【0263】

【数46】

$$\left| \sum_{k=\frac{1}{2}N+1}^N Q_{n_k} m_k(i_k, i_k) \right| - \left| \sum_{k=1}^{\frac{1}{2}N} Q_{n_k} m_k(i_k, i_k) \right| > T \quad \dots (6)$$

### 【0264】

本実施の形態では、4個の有意ビットQn<sub>1</sub>m<sub>1</sub>（i<sub>1</sub>，j<sub>1</sub>），Qn<sub>2</sub>m<sub>2</sub>（i<sub>2</sub>，j<sub>2</sub>），Qn<sub>3</sub>m<sub>3</sub>（i<sub>3</sub>，j<sub>3</sub>），Qn<sub>4</sub>m<sub>4</sub>（i<sub>4</sub>，j<sub>4</sub>）を使用して一組のビット情報を形成し、ステップS6で取得したHash値が奇数である場合に4個の有意ビットQn<sub>1</sub>m<sub>1</sub>（i<sub>1</sub>，j<sub>1</sub>），Qn<sub>2</sub>m<sub>2</sub>（i<sub>2</sub>，j<sub>2</sub>），Qn<sub>3</sub>m<sub>3</sub>（i<sub>3</sub>，j<sub>3</sub>），Qn<sub>4</sub>m<sub>4</sub>（i<sub>4</sub>，j<sub>4</sub>）で形成される情報と自然数Tとの関係が（17）式を満足するON状態となり、ステップS6で取得したHash値が偶数である場合に4個の有意ビットQn<sub>1</sub>m<sub>1</sub>（i<sub>1</sub>，j<sub>1</sub>）

,  $Q_{n_2 m_2}(i_2, j_2)$ ,  $Q_{n_3 m_3}(i_3, j_3)$ ,  $Q_{n_4 m_4}(i_4, j_4)$  で形成される情報と自然数  $T$  との関係が (18) 式を満足する OFF 状態となるように、有意ビットの ON/OFF を行なう。すなわち、4 個の有意ビット  $Q_{n_1 m_1}(i_1, j_1)$ ,  $Q_{n_2 m_2}(i_2, j_2)$ ,  $Q_{n_3 m_3}(i_3, j_3)$ ,  $Q_{n_4 m_4}(i_4, j_4)$  と、ある自然数  $T$  との関係が、(17) 式または (18) 式を満たすまで、以下の処理を繰り返す。

【0265】

【数 47】

$$|Q_{n_1 m_1}(i_1, j_1) + Q_{n_2 m_2}(i_2, j_2)| - |Q_{n_3 m_3}(i_3, j_3) + Q_{n_4 m_4}(i_4, j_4)| > T \quad \dots (17)$$

```
{
  if( 0 ≤ Qn3 m3(i3, j3) + Qn4 m4(i4, j4) )
  then
  {
    if( 2 ≤ Qn3 m3(i3, j3) + Qn4 m4(i4, j4) )
    {
      Qn3 m3(i3, j3) = Qn3 m3(i3, j3) - 1;
      Qn4 m4(i4, j4) = Qn4 m4(i4, j4) - 1;
    }
  }
  else
  {
    if( Qn3 m3(i3, j3) + Qn4 m4(i4, j4) ≤ -2 )
    {
      Qn3 m3(i3, j3) = Qn3 m3(i3, j3) + 1;
      Qn4 m4(i4, j4) = Qn4 m4(i4, j4) + 1;
    }
  }

  if( 0 ≤ Qn1 m1(i1, j1) + Qn2 m2(i2, j2) )
  then
  {
    Qn1 m1(i1, j1) = Qn1 m1(i1, j1) + 1;
    Qn2 m2(i2, j2) = Qn2 m2(i2, j2) + 1;
  }
  else
  {
    Qn1 m1(i1, j1) = Qn1 m1(i1, j1) - 1;
    Qn2 m2(i2, j2) = Qn2 m2(i2, j2) - 1;
  }
}
```

【0266】



## 【数 4 8】

$$|Q_{n_3 m_3}(i_3, j_3) + Q_{n_4 m_4}(i_4, j_4)| - |Q_{n_1 m_1}(i_1, j_1) + Q_{n_2 m_2}(i_2, j_2)| > T$$

... (18)

```

{
  if(0 ≤ Qn3m3(i3, j3) + Qn4m4(i4, j4))
  then
  {
    Qn3m3(i3, j3) = Qn3m3(i3, j3) + 1;
    Qn4m4(i4, j4) = Qn4m4(i4, j4) + 1;
  }
  else
  {
    Qn3m3(i3, j3) = Qn3m3(i3, j3) - 1;
    Qn4m4(i4, j4) = Qn4m4(i4, j4) - 1;
  }

  if(0 ≤ Qn1m1(i1, j1) + Qn2m2(i2, j2))
  then
  {
    if(2 ≤ Qn1m1(i1, j1) + Qn2m2(i2, j2))
    {
      Qn1m1(i1, j1) = Qn1m1(i1, j1) - 1;
      Qn2m2(i2, j2) = Qn2m2(i2, j2) - 1;
    }
  }
  else
  {
    if(Qn1m1(i1, j1) + Qn2m2(i2, j2) ≤ -2)
    {
      Qn1m1(i1, j1) = Qn1m1(i1, j1) + 1;
      Qn2m2(i2, j2) = Qn2m2(i2, j2) + 1;
    }
  }
}

```

## 【0 2 6 7】

また、本実施の形態の画像管理装置 1 は、図 9 に示すステップ S 2 8 に相当する処理として、 $n_i$  番目のブロック B L の  $m_j$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{n_i m_j}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が (5) 式を満足する ON 状態および (6) 式を満足する OFF 状態によって表わされる偶奇性と、 $n_i$  番目のブロック B L における H a s h 値の偶奇性と、が一致するか否かを判断する。ここに、流用検出手段および流用検出機能が実現される。

## 【0 2 6 8】

本実施の形態では、図 7 において、4 個の有意ビット  $Q_{n_1 m_1} (i_1, j_1)$ ,  $Q_{n_2 m_2} (i_2, j_2)$ ,  $Q_{n_3 m_3} (i_3, j_3)$ ,  $Q_{n_4 m_4} (i_4, j_4)$  を使用し、 $n$  番目のブロック  $BL$  の  $Hash$  値に応じて、 $n$  番目のブロック  $BL$  の  $m_j$  番目のビットプレーンにおける有意ビットの  $ON/OFF$  を調整したため、ステップ  $S28$  においても、4 個の有意ビット  $Q_{n_1 m_1} (i_1, j_1)$ ,  $Q_{n_2 m_2} (i_2, j_2)$ ,  $Q_{n_3 m_3} (i_3, j_3)$ ,  $Q_{n_4 m_4} (i_4, j_4)$  を使用する。

#### 【0269】

ステップ  $S28$  では、ステップ  $S26$  で取得した  $Hash$  値が奇数である場合に 4 個の有意ビット  $Q_{n_1 m_1} (i_1, j_1)$ ,  $Q_{n_2 m_2} (i_2, j_2)$ ,  $Q_{n_3 m_3} (i_3, j_3)$ ,  $Q_{n_4 m_4} (i_4, j_4)$  の関係が (19) 式を満足する  $ON$  状態となり、ステップ  $S26$  で取得した  $Hash$  値が偶数である場合に 4 個の有意ビット  $Q_{n_1 m_1} (i_1, j_1)$ ,  $Q_{n_2 m_2} (i_2, j_2)$ ,  $Q_{n_3 m_3} (i_3, j_3)$ ,  $Q_{n_4 m_4} (i_4, j_4)$  の関係が (20) 式を満足する  $OFF$  状態となるかを判断する。

$$\begin{aligned} & |Q_{n_1 m_1} (i_1, j_1) + Q_{n_2 m_2} (i_2, j_2)| \\ & > |Q_{n_3 m_3} (i_3, j_3) + Q_{n_4 m_4} (i_4, j_4)| \quad \cdots (19) \end{aligned}$$

$$\begin{aligned} & |Q_{n_1 m_1} (i_1, j_1) + Q_{n_2 m_2} (i_2, j_2)| \\ & < |Q_{n_3 m_3} (i_3, j_3) + Q_{n_4 m_4} (i_4, j_4)| \quad \cdots (20) \end{aligned}$$

#### 【0270】

本実施の形態によれば、複数のブロック  $BL$  の複数のビットプレーンの有意ビットを使用して電子透かしを埋め込むため、電子透かしを埋め込む場所がさらに分散されるので、画質の劣化を抑えて電子透かしの耐性をより強くするとともに、流用検出のための調査対象となる領域の分解能をさらに上げることができる。

#### 【0271】

次に、本発明の第 4 の実施の形態について図 10 および図 11 を参照して説明する。

#### 【0272】

図 10 は、本実施の形態の画像管理装置 1 による電子透かしの埋め込みに際し

て画像管理装置 1 が行なう動作について概略的に説明するフローチャートである。

#### 【0273】

本実施の形態では、図 10 に示すように、ステップ S 7 で、変更可能領域であると判断した場合には、変更可能領域内の処理対象箇所が間引き対象箇所であるか否かを判断する (S 15)。ここに、量子化係数選択手段および量子化係数選択機能が実現される。

#### 【0274】

ステップ S 15 では、例えば、処理対象箇所が予め設定された間引き対象箇所であるか否かを判断したり、隣り合う量子化係数との差が予め設定されたしきい値よりも大きいか否か等を判断したりすることによって、変更可能領域内の処理対象箇所が間引き対象箇所であるか否かを判断する。

#### 【0275】

変更可能領域内の処理対象箇所が間引き対象箇所であると判断した場合には (S 15 の Y)、ステップ S 8 に進み、間引き対象となる量子化係数から抽出した複数個の量子化係数  $Q_{nm}(x, y)$  の偶奇性を調整する。ここに、電子透かし埋め込み手段および電子透かし埋め込み機能が実現される。

#### 【0276】

一方、変更可能領域内の処理対象箇所が間引き対象箇所ではないと判断した場合には (S 15 の N)、ステップ S 9 に進む。

#### 【0277】

本実施の形態によれば、量子化係数  $Q_{nm}(x, y)$  に対して選択的に電子透かしを埋め込むことにより、全ての量子化係数に電子透かしを埋め込む場合と比較して、電子透かしを埋め込むことによる画質劣化を抑えることができる。

#### 【0278】

このとき、隣り合う量子化係数に対する変化が激しい (急激に変化する)、すなわち、エッジ部に相当するの量子化係数を、処理対象として選択することにより、全ての量子化係数に電子透かしを埋め込む場合と比較して画質劣化を抑えるとともに、電子透かしを埋め込むことによる画質劣化を目立ち難くして、電子透

かしを埋め込むことによる画質劣化を効果的に抑えることができる。

#### 【0279】

また、単一のブロック BL において、処理対象として選択する量子化係数の選択頻度は調整可能であるため、電子透かしの埋め込みにおける処理における処理量や処理速度等を調整することができる。

#### 【0280】

加えて、本実施の形態では、電子透かしの埋め込みに加えて、ステップ S15 で用いたしきい値を埋め込む。ここに、しきい値埋め込み手段としての機能が実現される。公知の技術であるため説明を省略するが、量子化係数に対するしきい値の埋め込みは、電子透かしの埋め込みと同様に、特定のビットの ON/OFF によって行なう。

#### 【0281】

図 11 は、電子透かしが埋め込まれた符号列データの流用検出に際して画像処理装置が行なう動作について概略的に説明するフローチャートである。

#### 【0282】

本実施の形態では、図 11 に示すように、 $n$  番目のブロック BL における対象とする量子化係数が変更可能領域にあると判断した場合には (S27 の Y)、変更可能領域内の処理対象となる量子化係数が間引き対象となっているか否かを判断し (S35)、変更可能領域内の処理対象となる量子化係数が間引き対象となっていると判断した場合には (S35 の Y)、ステップ S28 に進み、 $n$  番目のブロック BL の  $m$  番目のビットプレーンの  $N$  ( $N$  は偶数) 個の有意ビット  $Q_{nm}(x, y)$  ( $x = 0, 1, \dots; y = 0, 1, \dots$ ) によって形成される情報と自然数  $T$  との関係が (7) 式を満足する ON 状態および (8) 式を満足する OFF 状態によって表わされる偶奇性と、 $n$  番目のブロックにおける Hash 値の偶奇性と、が一致するか否かを判断する。ここに、流用検出手段および流用検出機能が実現される。

#### 【0283】

一方、変更可能領域内の処理対象となる量子化係数が間引き対象ではないと判断した場合には (S35 の N)、ステップ S30 に進む。

## 【0284】

なお、本実施の形態では、第1の実施の形態の方法で電子透かしを埋め込み、第1の実施の形態の方法で流用を検出するようにしたが、これに限るものではなく、第2、第3の実施の形態の方法で電子透かしを埋め込み、第2、第3の実施の形態の方法で流用を検出するようにしてもよい。

## 【0285】

## 【発明の効果】

請求項1記載の発明の符号生成装置によれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがなく、単一のビットプレーン内の有意ビットに対してON/OFF調整するため、符号化に際してビットプレーン単位の切り捨てがあった場合にも、有意ビットのON/OFFによって埋め込まれる電子透かしを消滅させることがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項20記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができる。

## 【0286】

請求項2記載の発明の符号生成装置によれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項20記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができることに加えて、ON/OFF調整する有意ビットを複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を抑制するとともに、流用の検出に際しての対象領域の分解能を上げることができる。

## 【0287】

請求項3記載の発明の符号生成装置によれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項20記載の発明の画像処理装置を用いることにより、画像の流用をブロック単位で検出することができることに加えて、ON/OFF調整する有意ビットを複数のブロックの複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を効果的に抑制するとともに、流用の検出に際しての対象領域の分解能をより上げることができる。

#### 【0288】

請求項4記載の発明によれば、請求項1ないし3のいずれかーに記載の符号生成装置において、第1の方式または第2の方式の2つの方式のうちいずれか一方を選択的に用いることにより、埋め込まれる電子透かしを、効果的に第三者に解読し難くすることができる。

#### 【0289】

請求項5記載の発明によれば、請求項4記載の符号生成装置において、第1の方式または第2の方式を切替自在に設定することができる。

#### 【0290】

請求項6記載の発明によれば、請求項5記載の符号生成装置において、符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0291】

請求項7記載の発明によれば、請求項5記載の符号生成装置において、秘密情報が入力された場合には、符号化ハッシュ値と秘密情報とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0292】

請求項 8 記載の発明によれば、請求項 1 ないし 7 のいずれかーに記載の符号生成装置において、ビットプレーンの上位から下位方向への符号化においてビットの ON/OFF を均等に行ない、電子透かしを埋め込むことによる（有意ビットの ON/OFF による）画質劣化を抑えることができる。

【0293】

請求項 9 記載の発明によれば、請求項 1 ないし 8 のいずれかーに記載の符号生成装置において、全ての有意ビットを ON/OFF 調整を行なう場合と比較して、電子透かしを埋め込むことによる画質劣化を抑えることができる。

【0294】

請求項 10 記載の発明によれば、請求項 9 記載の符号生成装置において、隣り合う量子化係数との差がしきい値以上である、すなわち、隣り合う量子化係数に対して変化の激しい量子化係数における有意ビットを ON/OFF することにより、電子透かしを埋め込むことによる画質劣化をより効果的に抑えることができる。

【0295】

請求項 11 記載の発明によれば、請求項 10 記載の符号生成装置において、例えば、画質劣化程度や流用の検出精度等に応じて、使用目的に応じたしきい値を設定することができる。

【0296】

請求項 12 記載の発明によれば、請求項 10 または 11 記載の符号生成装置において、例えば、請求項 20 記載の発明の画像処理装置を用いて、符号列データ中に埋め込んだしきい値を復元して活用することができる。

【0297】

請求項 13 記載の発明によれば、請求項 9 ないし 12 のいずれかーに記載の符号生成装置において、例えば、目的とする画質程度等に応じた頻度で量子化係数を取得することにより、電子透かしを埋め込むことによる画質劣化の程度を管理することができる。

【0298】

請求項 14 記載の発明によれば、請求項 1 ないし 13 のいずれかーに記載の符

号生成装置において、量子化係数に加えて秘密情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

【0299】

請求項15記載の発明によれば、請求項1ないし13のいずれかーに記載の符号生成装置において、量子化係数に加えて日付情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

【0300】

請求項16記載の発明によれば、請求項1ないし13のいずれかーに記載の符号生成装置において、量子化係数に加えて製造番号に基づく情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

【0301】

請求項17記載の発明によれば、請求項1ないし13のいずれかーに記載の符号生成装置において、量子化係数に加えて、秘密情報、日付情報、製造番号に基づく情報のうち二つ以上の情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

【0302】

請求項18記載の発明によれば、請求項17記載の符号生成装置において、例えば、ユーザ等が選択した任意の情報をハッシュ変換の種とすることができ、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

【0303】

請求項19記載の発明によれば、請求項1ないし18のいずれかーに記載の符号生成装置において、例えば、デジタルカメラやスキャナ等の入力手段を用いて入力した画像に電子透かしを埋め込むことができる。

【0304】

請求項20記載の発明の画像処理装置によれば、請求項1ないし19のいずれかーに記載の符号生成装置が生成した符号列データを流用した画像であることを検出することができる。

【0305】



請求項 21 記載の発明によれば、請求項 20 記載の発明の画像処理装置において、流用された画像である場合、流用された画像であることを流用されたブロック単位で視認させることができる。

#### 【0306】

請求項 22 記載の発明によれば、請求項 21 記載の画像処理装置において、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

#### 【0307】

請求項 23 記載の発明によれば、請求項 21 記載の画像処理装置において、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

#### 【0308】

請求項 24 記載の発明の符号生成プログラムによれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがなく、単一のビットプレーン内の有意ビットに対して ON/OFF 調整するため、符号化に際してビットプレーン単位の切り捨てがあった場合にも、有意ビットの ON/OFF によって埋め込まれる電子透かしを消滅させることがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットの ON/OFF 調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項 42 記載の発明の画像処理プログラムを実行することにより、画像の流用をブロック単位で検出することができる。

#### 【0309】

請求項 25 記載の発明の符号生成プログラムによれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットの ON/OFF 調整に用いる符号化ハッシュ値をブロック単位で取得するため、例えば、画像が流用された場合にも、請求項 42 記載の発明の画像処理プログラムを実行することにより、

より、画像の流用をブロック単位で検出することができることに加えて、ON/OFF調整する有意ビットを複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を抑制するとともに、流用の検出に際しての対象領域の分解能を上げることができる。

#### 【0310】

請求項26記載の発明の符号生成プログラムによれば、量子化係数に電子透かしを埋め込むことにより画像データの符号化、復号化を繰り返しても埋め込んだ電子透かしが劣化してしまうことがないので、符号化、復号化を繰り返しても流用の検出を精度よく行なうことができる。また、有意ビットのON/OFF調整に用いる符号化ハッシュ値をブロック単位で取得するため、画像が流用された場合にも、請求項42記載の発明の画像処理プログラムを実行することにより、画像の流用をブロック単位で検出することができることに加えて、ON/OFF調整する有意ビットを複数のブロックの複数のビットプレーンに分散することにより、電子透かしを埋め込むことによる画質劣化を効果的に抑制するとともに、流用の検出に際しての対象領域の分解能をより上げることができる。

#### 【0311】

請求項27記載の発明によれば、請求項24ないし26のいずれかに記載の符号生成プログラムにおいて、第1の方式または第2の方式の2つの方式のうちいずれか一方を選択的に用いることにより、埋め込まれる電子透かしを、効果的に第三者に解読し難くすることができる。

#### 【0312】

請求項28記載の発明によれば、請求項27記載の符号生成プログラムにおいて、第1の方式または第2の方式を切替自在に設定することができる。

#### 【0313】

請求項29記載の発明によれば、請求項28記載の符号生成プログラムにおいて、符号化ハッシュ値と処理対象となる前記量子化係数の画像中での座標値とに基づいて第1の方式または第2の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0314】

請求項 3 0 記載の発明によれば、請求項 2 8 記載の符号生成プログラムにおいて、秘密情報が入力された場合には、符号化ハッシュ値と秘密情報とに基づいて第 1 の方式または第 2 の方式を設定することにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【 0 3 1 5 】

請求項 3 1 記載の発明によれば、請求項 2 4 ないし 3 0 のいずれか一に記載の符号生成プログラムにおいて、ビットプレーンの上位から下位方向への符号化においてビットの ON / OFF が均等に行ない、電子透かしを埋め込むことによる画質劣化を抑えることができる。

#### 【 0 3 1 6 】

請求項 3 2 記載の発明によれば、請求項 2 4 ないし 3 1 のいずれか一に記載の符号生成プログラムにおいて、全ての有意ビットを ON / OFF 調整を行なう場合と比較して電子透かしを埋め込むことによる画質劣化を抑えることができる。

#### 【 0 3 1 7 】

請求項 3 3 記載の発明によれば、請求項 3 2 記載の符号生成プログラムにおいて、隣り合う量子化係数に対して変化の激しい量子化係数における有意ビットを ON / OFF することにより、電子透かしを埋め込むことによる画質劣化をより効果的に抑えることができる。

#### 【 0 3 1 8 】

請求項 3 4 記載の発明によれば、請求項 3 3 記載の符号生成プログラムにおいて、例えば、画質劣化程度や流用の検出精度等に応じて、使用目的に応じたしきい値を設定することができる。

#### 【 0 3 1 9 】

請求項 3 5 記載の発明によれば、請求項 3 3 または 3 4 記載の符号生成プログラムにおいて、例えば、請求項 4 2 記載の発明の画像処理プログラムを実行する際に、符号列データ中に埋め込んだしきい値を復元して活用することができる。

#### 【 0 3 2 0 】

請求項 3 6 記載の発明によれば、請求項 3 2 ないし 3 5 のいずれか一に記載の符号生成プログラムにおいて、例えば、目的とする画質程度等に応じた頻度で量

子化係数を取得することにより、電子透かしを埋め込むことによる画質劣化の程度を管理することができる。

#### 【0321】

請求項37記載の発明によれば、請求項24ないし36のいずれかに記載の符号生成プログラムにおいて、各ブロックの量子化係数に加えて外部から入力された秘密情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0322】

請求項38記載の発明によれば、請求項24ないし36のいずれかに記載の符号生成プログラムにおいて、各ブロックの量子化係数に加えて日付情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0323】

請求項39記載の発明によれば、請求項24ないし36のいずれかに記載の符号生成プログラムにおいて、各ブロックの量子化係数に加えて製造番号に基づく情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを第三者に解読し難くすることができる。

#### 【0324】

請求項40記載の発明によれば、請求項24ないし36のいずれかに記載の符号生成プログラムにおいて、各ブロックの量子化係数に加えて、外部から入力された秘密情報、日付情報、製造番号に基づく情報のうち二つ以上の情報をハッシュ変換の種とすることにより、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0325】

請求項41記載の発明によれば、請求項40記載の符号生成プログラムにおいて、例えば、ユーザ等が選択した任意の情報をハッシュ変換の種とすることができ、埋め込まれる電子透かしを、より効果的に第三者に解読し難くすることができる。

#### 【0326】

請求項 4 2 記載の発明の画像処理プログラムによれば、請求項 2 4 ないし 4 1 のいずれかに記載の符号生成プログラムの実行により生成した符号列データを流用した画像であることを検出することができる。

【0327】

請求項 4 3 記載の発明によれば、請求項 4 2 記載の画像処理プログラムにおいて、流用された画像である場合、流用された画像であることを流用されたブロック単位で視認させることができる。

【0328】

請求項 4 4 記載の発明によれば、請求項 4 3 記載の画像処理プログラムにおいて、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

【0329】

請求項 4 5 記載の発明によれば、請求項 4 3 記載の画像処理プログラムにおいて、流用された画像である場合、実用上、容易に流用されたブロックを視覚させることができる。

【0330】

請求項 4 6 記載の発明の記憶媒体によれば、請求項 2 4 ないし 4 1 のいずれかに記載の発明の効果をを得ることができる。

【0331】

請求項 4 7 記載の発明の記憶媒体によれば、請求項 4 2 ないし 4 5 のいずれかに記載の発明の作用を得ることができる。

【図面の簡単な説明】

【図 1】

J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを示す説明図である。

【図 2】

原画像の各コンポーネントの分割された矩形領域を示す説明図である。

【図 3】

デコンポジションレベル数が 3 の場合の、各デコンポジションレベルにおける

サブバンドを示す説明図である。

【図 4】

プリシントを示す説明図である。

【図 5】

ビットプレーンに順位付けする手順の一例を示す説明図である。

【図 6】

本発明の第 1 の実施の形態の画像処理装置の構成を概略的に説明するブロック図である。

【図 7】

電子透かしの埋め込みに際して画像処理装置が行なう動作について概略的に説明するフローチャートである。

【図 8】

ブロック分割を示す説明図である。

【図 9】

電子透かしが埋め込まれた符号列データの改ざん検出に際して画像処理装置が行なう動作について概略的に説明するフローチャートである。

【図 10】

本発明の第 4 の実施の形態の画像処理装置による電子透かしの埋め込みに際して画像処理装置が行なう動作について概略的に説明するフローチャートである。

【図 11】

電子透かしが埋め込まれた符号列データの改ざん検出に際して画像処理装置が行なう動作について概略的に説明するフローチャートである。

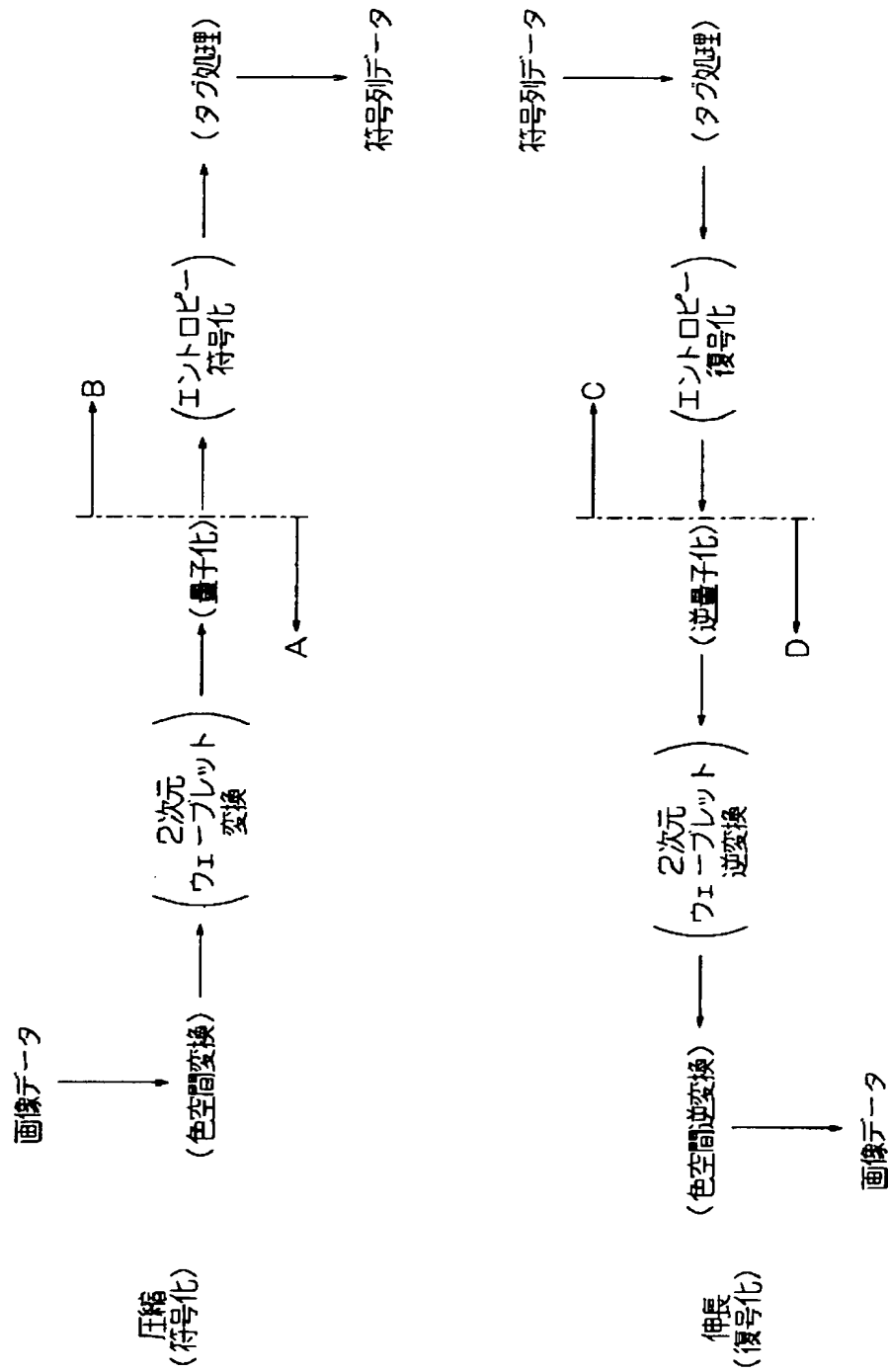
【符号の説明】

- 1        符号生成装置、画像処理装置
- 3        画像入力手段
- 5        表示部
- 18       記憶媒体



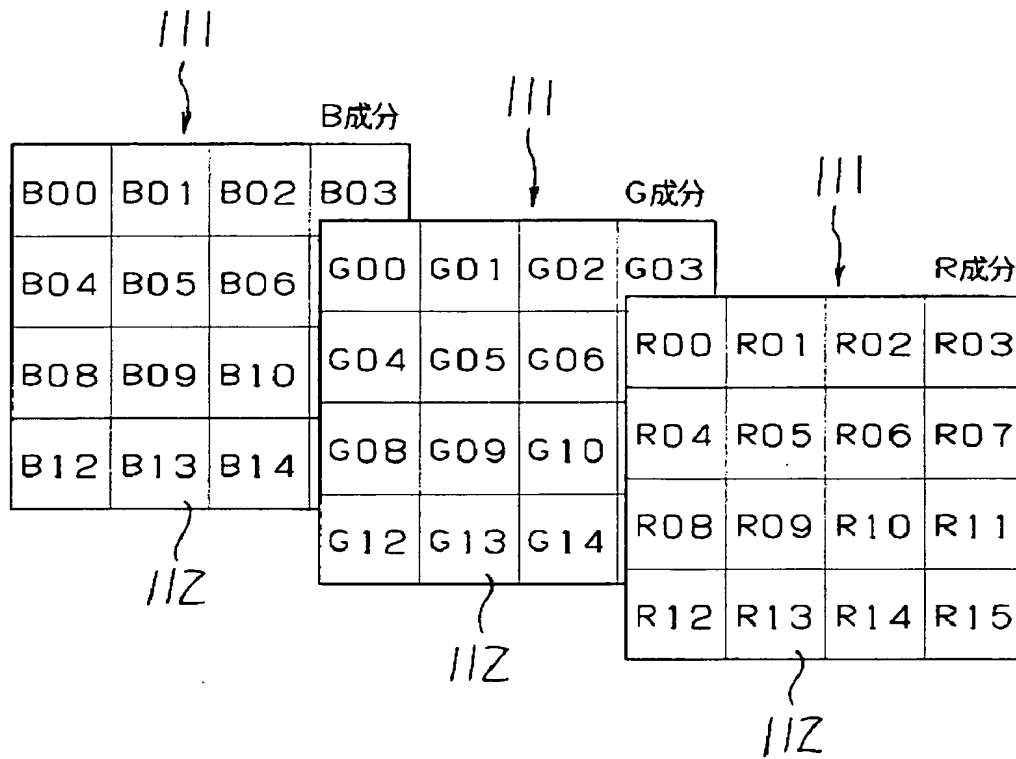
【書類名】 図面

【図 1】

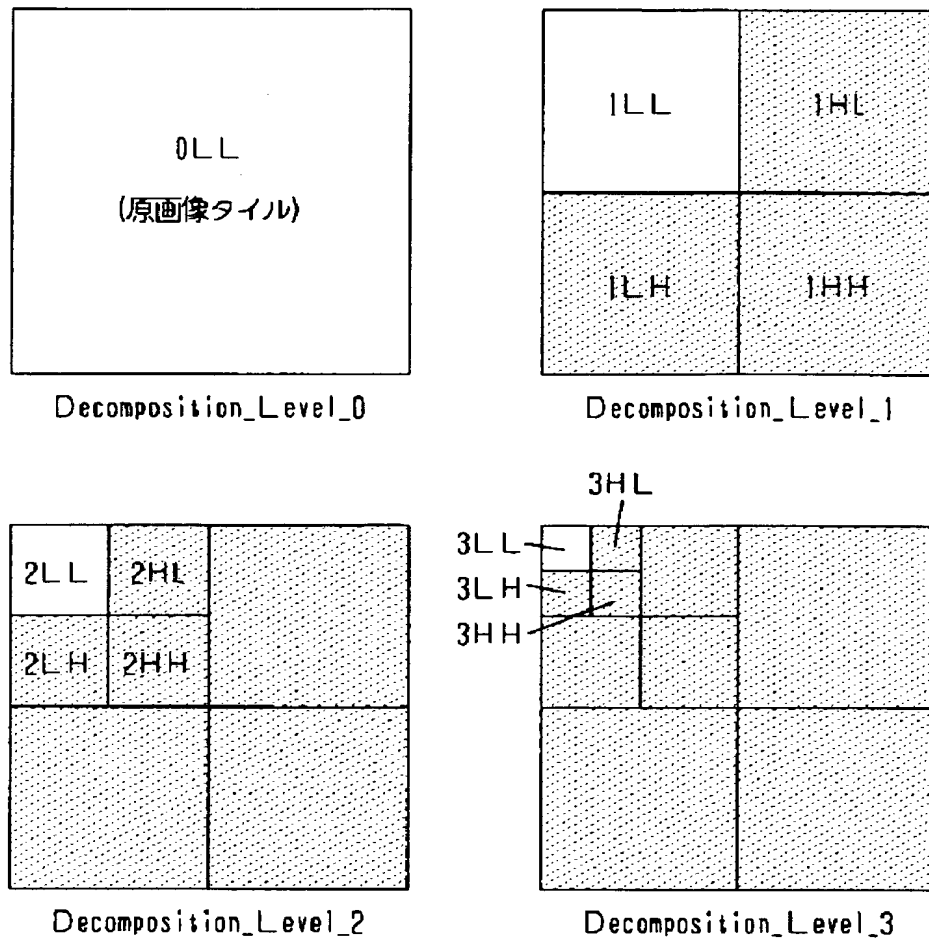




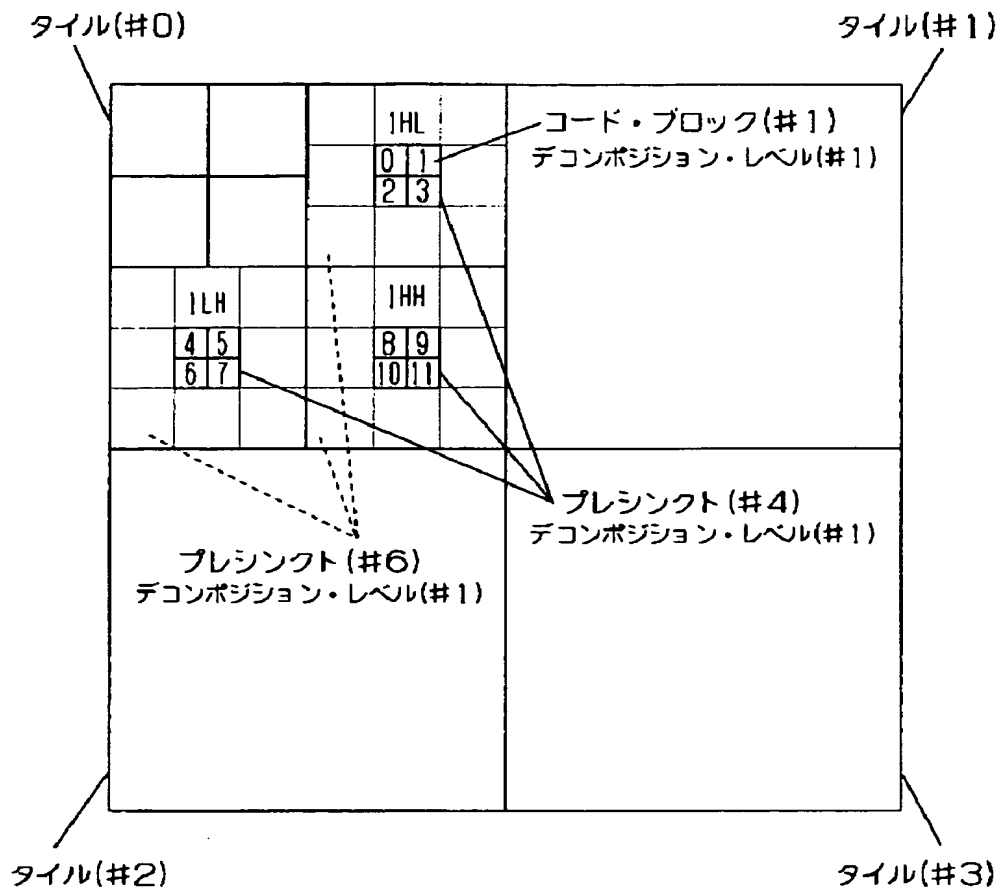
【図 2】



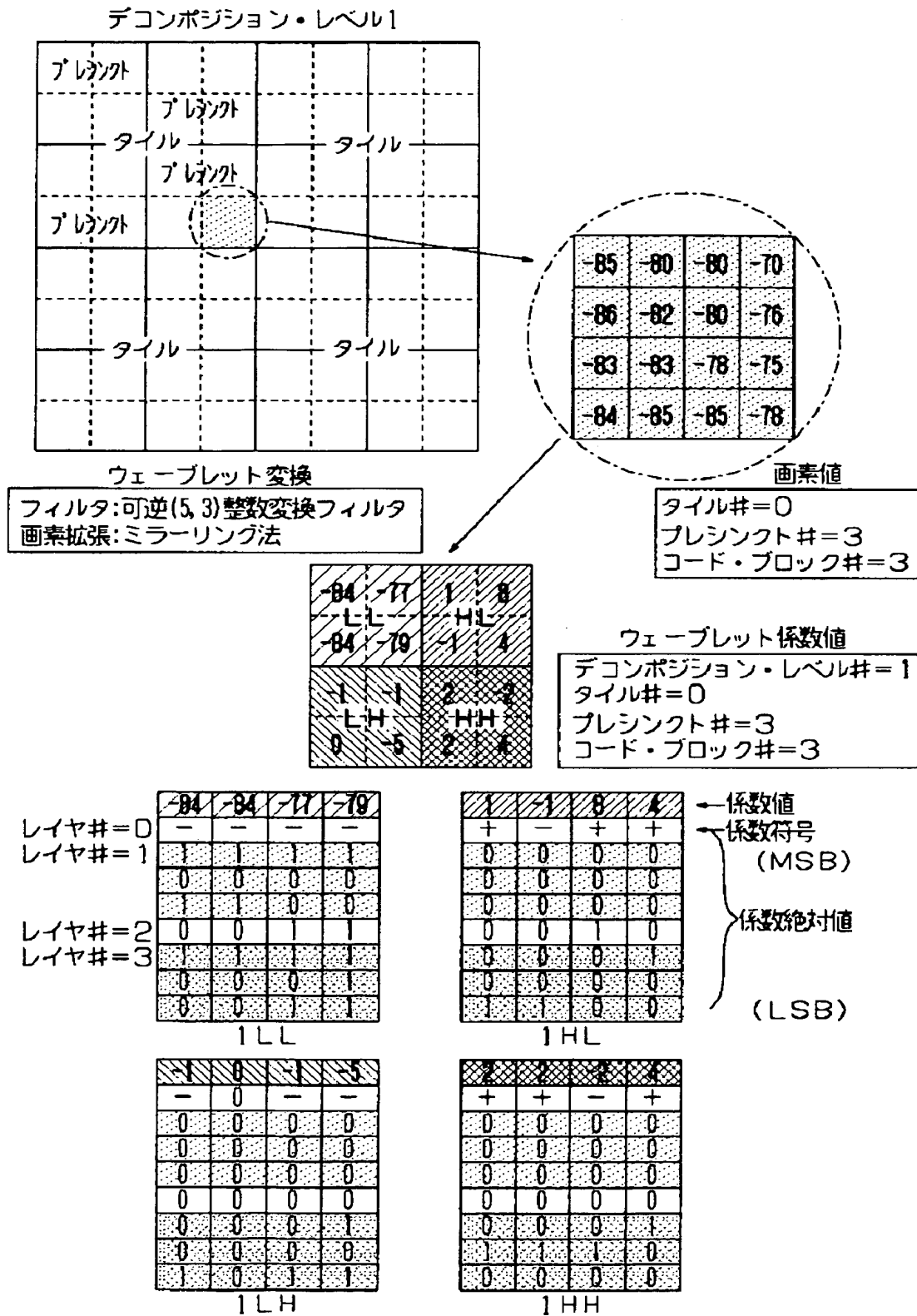
【図3】



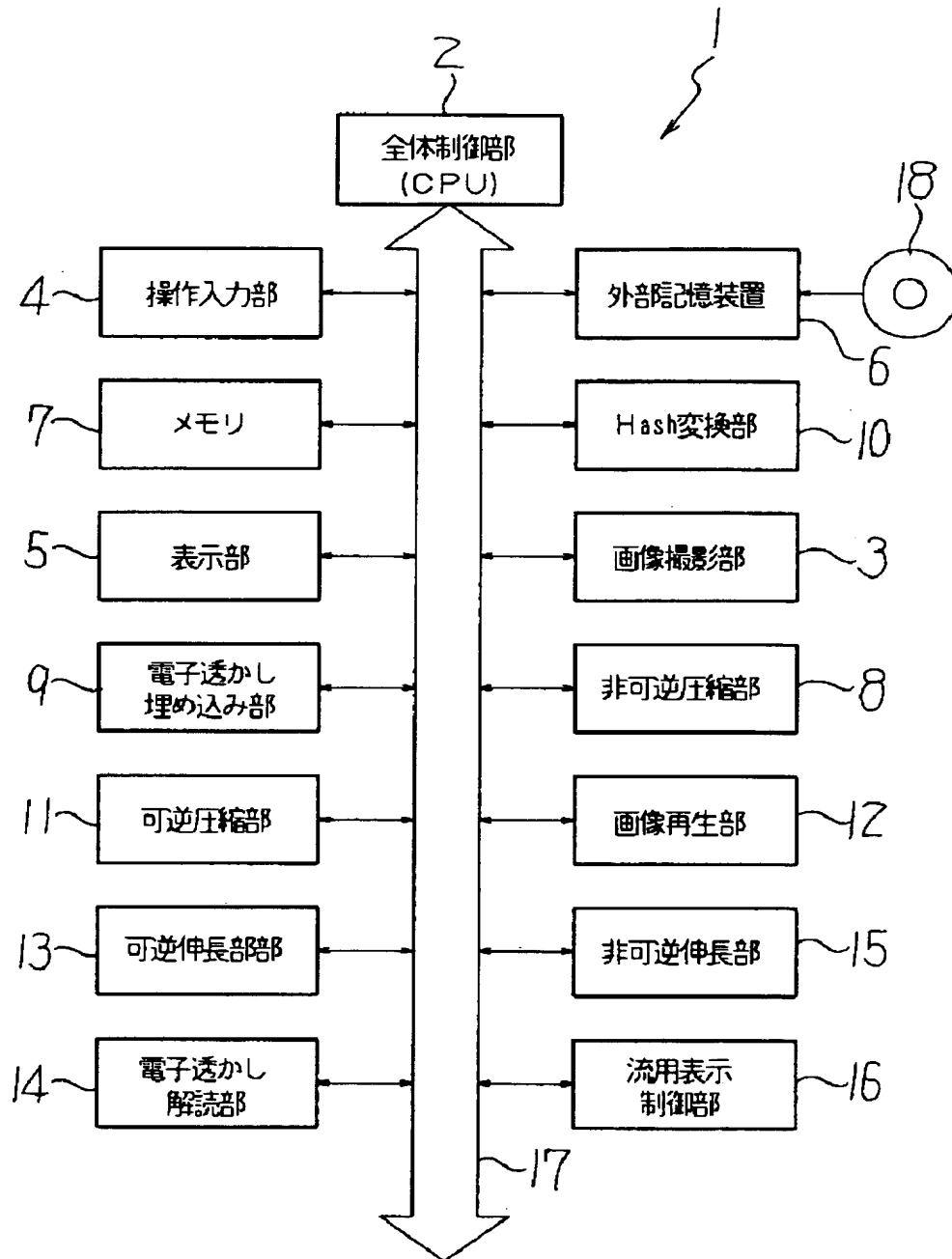
【図 4】



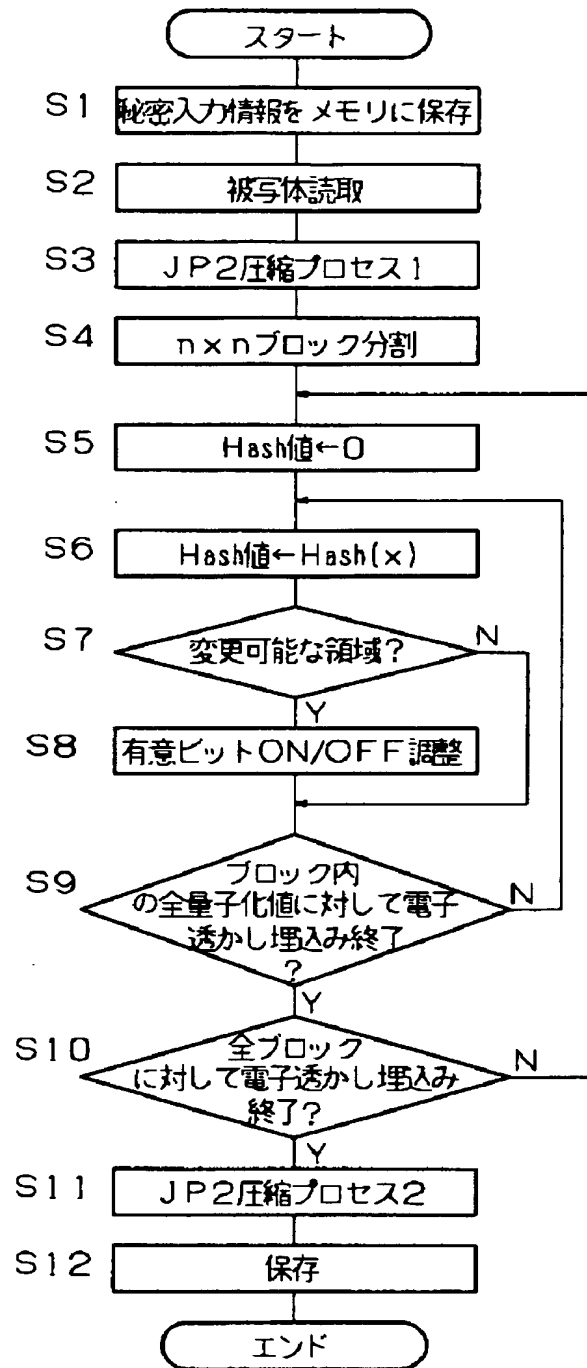
【図 5】



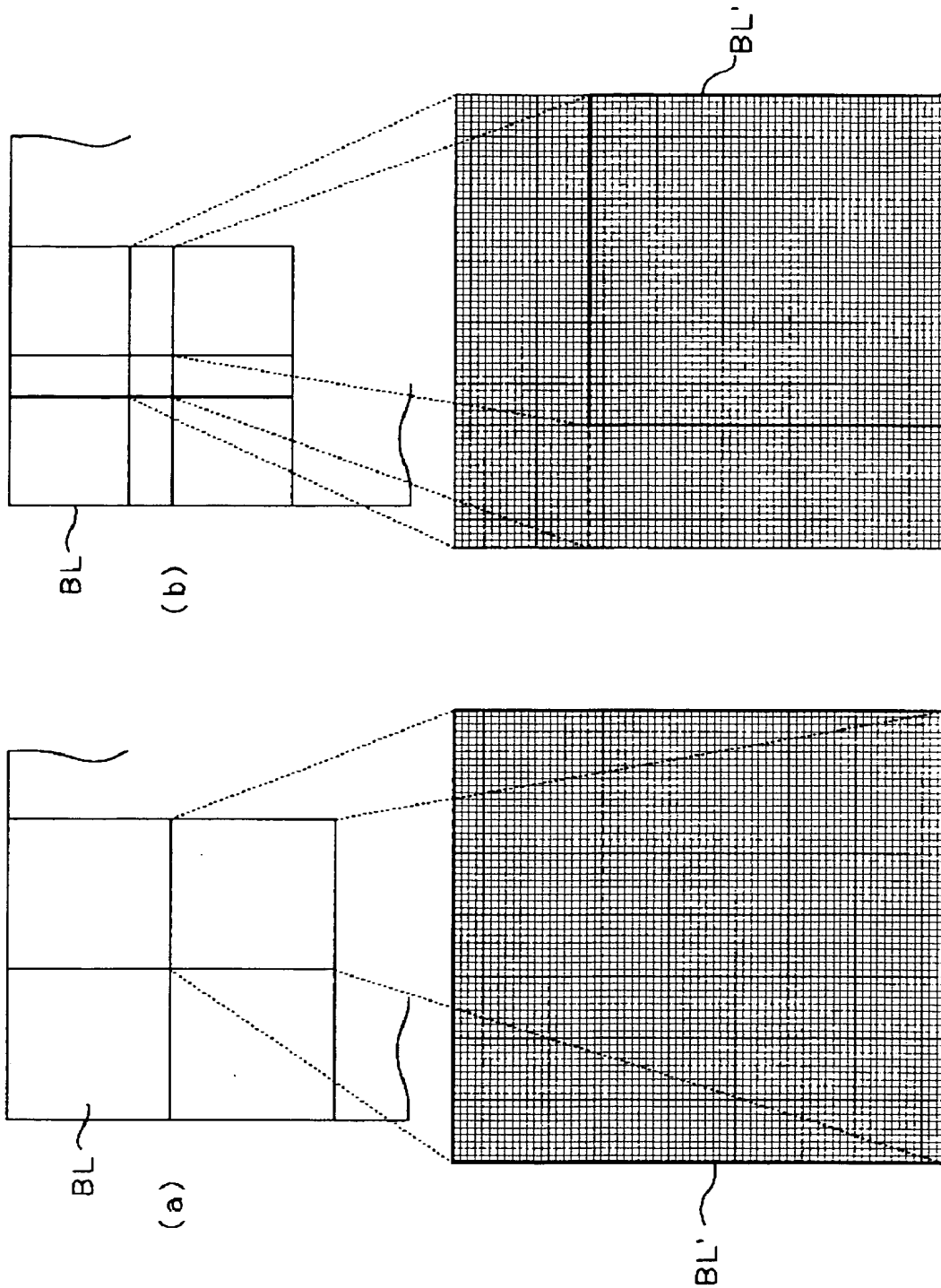
【図 6】



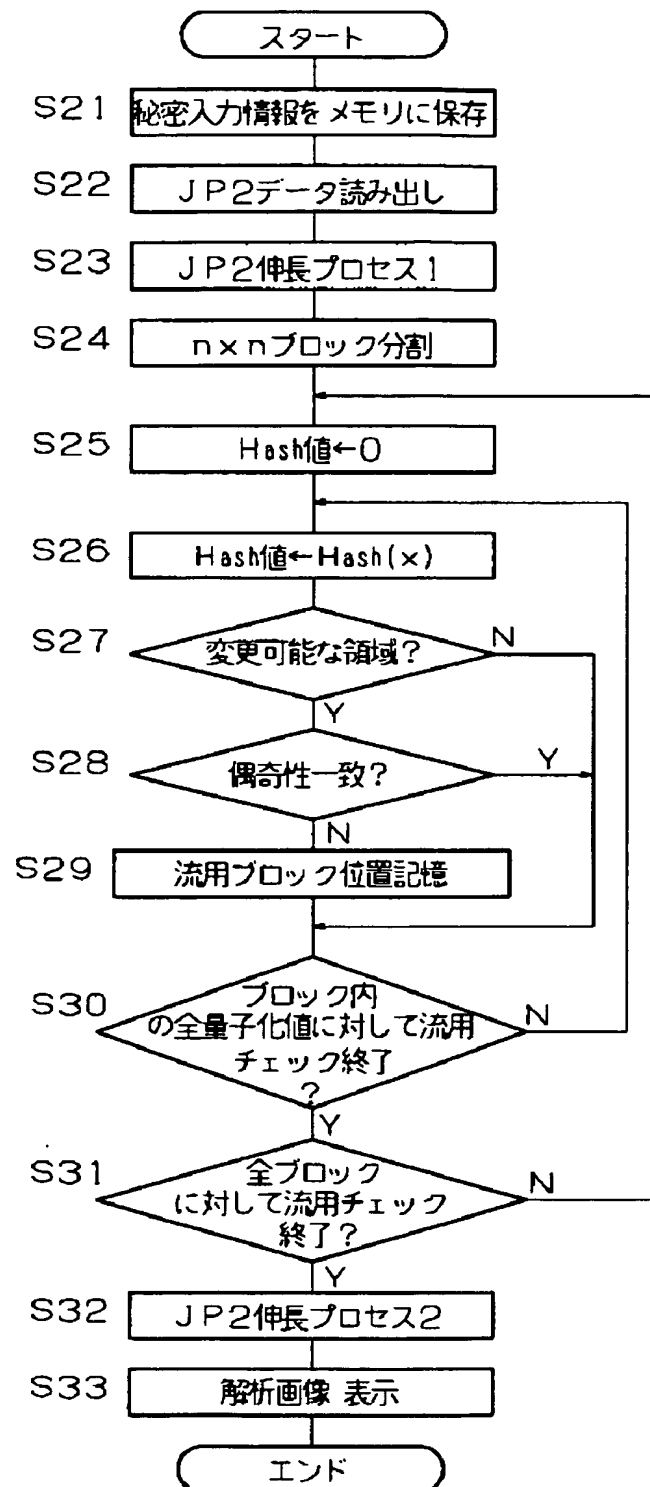
【図 7】



【図 8】

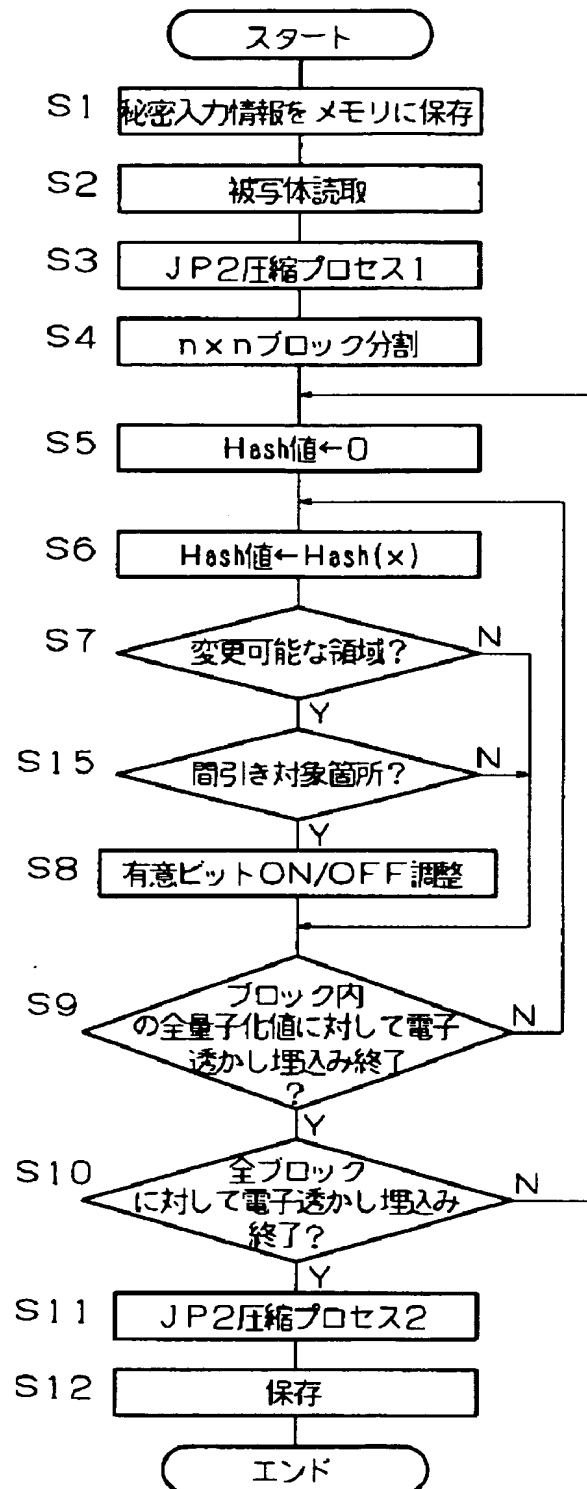


【図 9】

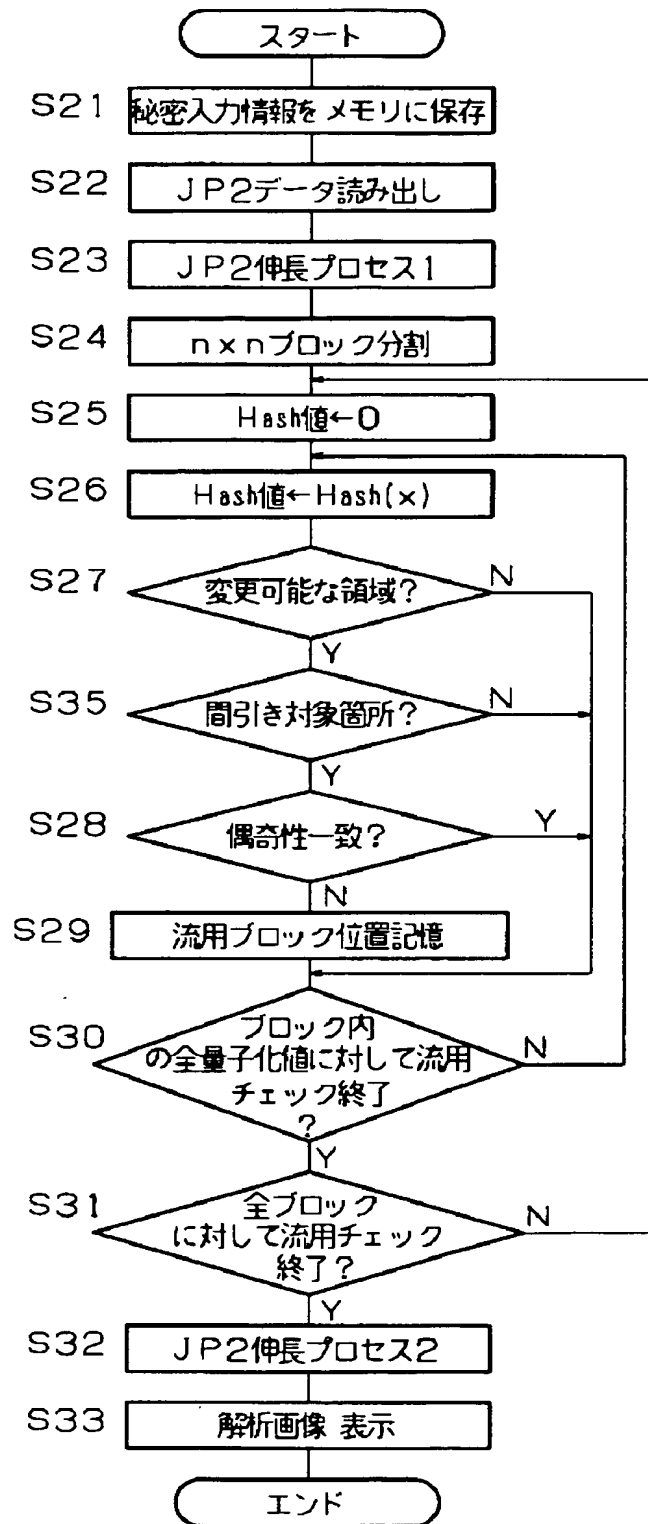




【図 10】



【図 11】





【書類名】 要約書

【要約】

【課題】 符号化、復号化を繰り返しても流用された画像であることを検出できるようにする。

【解決手段】 ステップ S 3 で画像を離散ウェーブレット変換して量子化した量子化係数をステップ S 4 でブロック単位に分割し、n 番目のブロックの量子化係数に基づいてハッシュ変換を行なってステップ S 6 で取得した符号化ハッシュ値の偶奇性に応じて、n 番目のブロックをビットプレーン単位に分割した m 番目のビットプレーンの N (N は偶数) 個の有意ビット  $Q_{nm}(x, y)$  によって形成される情報と自然数 T との関係が、(1) 式で表わされる ON 状態または (2) 式で表わされる OFF 状態を満足するようにステップ S 8 で有意ビットの ON/OFF を調整して電子透かしを埋め込んだ量子化係数を、ステップ S 11 で符号化して符号列データを生成するようにした。

【選択図】 図 7

特願 2002-338118

出 願 人 履 歴 情 報

識別番号

[000006747]

1. 変更年月日  
[変更理由]

2002年 5月17日

住所変更

住 所  
氏 名

東京都大田区中馬込1丁目3番6号  
株式会社リコー